BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-293724
(43)Date of publication of application : 04.11.1998

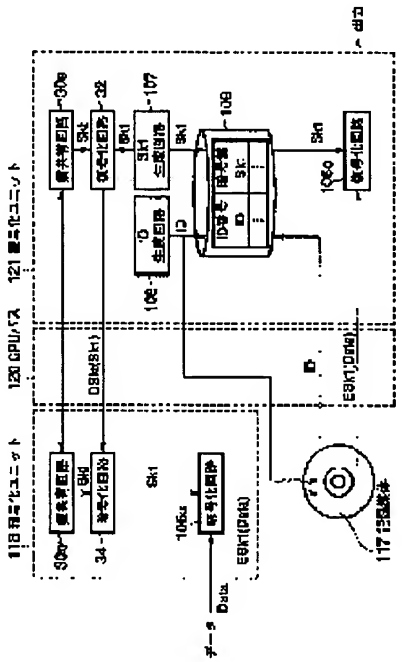
(51)Int.Cl. G06F 12/14
G09C 1/00
H04L 9/08
H04L 9/10

(21)Application number : 09-102055
(22)Date of filing : 18.04.1997

(71)Applicant : TOSHIBA CORP
(72)Inventor : KATO TAKEHISA
ENDO NAOKI

(54) UNIT DEVICE, DECODING UNIT DEVICE, CIPHERING UNIT DEVICE, CIPHERING SYSTEM, CIPHERING METHOD AND DECODING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent unauthorized copying by a third person by recording a data ciphering key generated every time inside a unit corresponding to identification information.
SOLUTION: This system is provided with a ciphering unit 118 and a decoding unit 121 and the ciphering unit 118 and the decoding unit 121 are connected to the CPU bus 120 of a personal computer. Then, at the time of ciphering one set of data, the data ciphering key Sk1 used for the ciphering of the data is generated, a pair with the identification information ID is generated, the pair is recorded in a database and the information of the ID and the data ciphered by the Sk1 are recorded in a recording medium 117. Then, at the time of reproduction, the data ciphering key Sk1 is obtained from the database based on the information of the ID read from the recording medium 117 and the ciphered data recorded in the recording medium 117 are decoded with the data ciphering key Sk1 as a decoding key.



LEGAL STATUS

[Date of request for examination] 11.09.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10293724 A**

(43) Date of publication of application: **04 . 11 . 98**

(51) Int. Cl **G06F 12/14**
G09C 1/00
H04L 9/08
H04L 9/10

(21) Application number: **09102055**

(22) Date of filing: **18 . 04 . 97**

(71) Applicant: **TOSHIBA CORP**

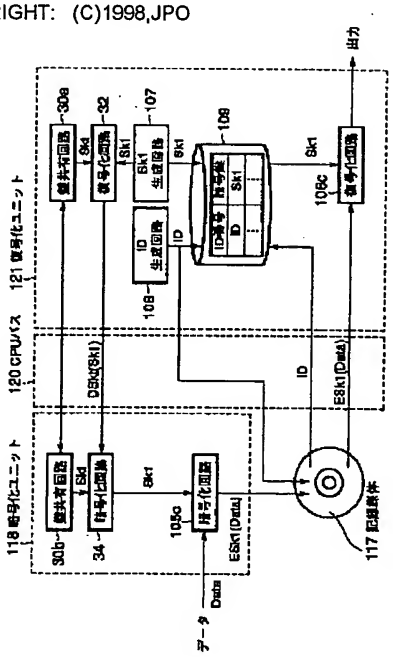
(72) Inventor: **KATO TAKEHISA**
ENDO NAOKI

(54) **UNIT DEVICE, DECODING UNIT DEVICE, CIPHERING UNIT DEVICE, CIPHERING SYSTEM, CIPHERING METHOD AND DECODING METHOD**

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent unauthorized copying by a third person by recording a data ciphering key generated every time inside a unit corresponding to identification information.

SOLUTION: This system is provided with a ciphering unit 118 and a decoding unit 121 and the ciphering unit 118 and the decoding unit 121 are connected to the CPU bus 120 of a personal computer. Then, at the time of ciphering one set of data, the data ciphering key Sk1 used for the ciphering of the data is generated, a pair with the identification information ID is generated, the pair is recorded in a database and the information of the ID and the data ciphered by the Sk1 are recorded in a recording medium 117. Then, at the time of reproduction, the data ciphering key Sk1 is obtained from the database based on the information of the ID read from the recording medium 117 and the ciphered data recorded in the recording medium 117 are decoded with the data ciphering key Sk1 as a decoding key.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－293724

(43)公開日　平成10年(1998)11月４日

(51)Int.Cl.[6]		識別記号		F I		
G06F	12/14	320		G06F	12/14	320B
G09C	1/00	660		G09C	1/00	660A
H04L	9/08			H04L	9/00	601A
	9/10					621A

審査請求　未請求　請求項の数14　ＯＬ　（全 26 頁）

(21)出願番号　特願平9－102055

(22)出願日　平成９年(1997)４月18日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　加藤　岳久
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　遠藤　直樹
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

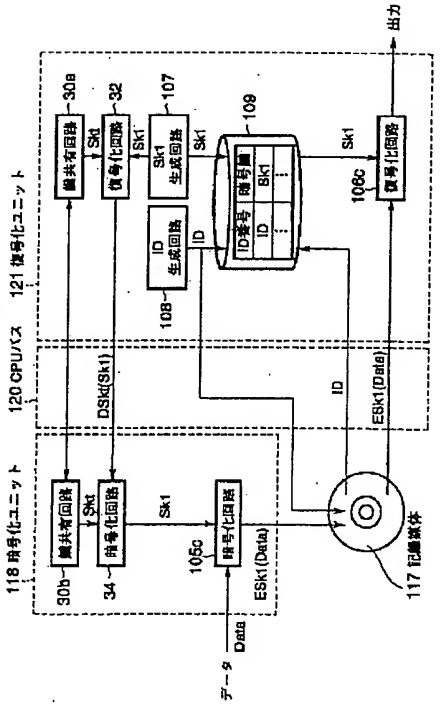
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　ユニット装置、復号化ユニット装置、暗号化ユニット装置、暗号処理システム、暗号化方法及び復号化方法

(57)【要約】

【課題】　第三者による不正コピーを防止可能な復号化装置を提供すること。

【解決手段】　記録媒体に記録された暗号化データを復号するＣＰＵバスに接続される復号化装置であって、ＣＰＵバスを介さずに入力されたデータを暗号化する暗号化装置が対象とするデータの識別番号と該データのための暗号鍵を生成するための手段と、暗号鍵と識別番号を対応付けて記録するための手段と、ＣＰＵバスを介して暗号化装置に暗号鍵を外部から取得されることなく安全に伝えるための手段と、自装置内に識別情報と対応して記録されている暗号鍵のうちから、識別情報とこれに対応する暗号鍵で暗号化されたデータが記録された記録媒体から読み出されＣＰＵバスを介して与えられた識別情報に対応する暗号鍵を求め、該暗号鍵を復号鍵として記録媒体から読み出されＣＰＵバスを介して与えられた暗号化データを復号するための手段とを備えたことを特徴とする。



1

【特許請求の範囲】

【請求項１】計算機のＣＰＵバスを介さずに入力したデータを所定の記録媒体に記録する前に暗号化する装置のために、データ暗号化鍵を生成し記録する、計算機のＣＰＵバスに接続されて使用されるユニット装置であって、

暗号化対象となるデータの識別番号を生成するための手段と、

前記データの暗号化に用いるデータ暗号化鍵を生成するための手段と、

生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、

前記計算機のＣＰＵバスを介して前記暗号化する装置に前記データ暗号化鍵または前記データ暗号化鍵と前記識別情報の両方を外部から取得されることなく安全に伝えるための手段とを備えたことを特徴とするユニット装置。

【請求項２】暗号化されて所定の記録媒体に記録されたデータを復号する、計算機のＣＰＵバスに接続されて使用される復号化ユニット装置であって、

前記計算機のＣＰＵバスを介さずに入力されたデータを暗号化する暗号化ユニット装置が暗号化対象とするデータの識別番号を生成するための手段と、

前記暗号化ユニット装置が前記データの暗号化に用いるデータ暗号化鍵を生成するための手段と、

生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、

前記計算機のＣＰＵバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段と、

自装置内に識別情報と対応して記録されているデータ暗号化鍵のうちから、識別情報とこれに対応するデータ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた識別情報に対応するデータ暗号化鍵を求めるための手段と、

求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化されたデータを復号するための手段とを備えたことを特徴とする復号化ユニット装置。

【請求項３】暗号化されて所定の記録媒体に記録されたデータを復号する、計算機のＣＰＵバスに接続されて使用される復号化ユニット装置であって、

前記計算機のＣＰＵバスを介さずに入力されたデータを暗号化する暗号化ユニット装置が暗号化対象とするデータの識別番号を生成するための手段と、

前記暗号化ユニット装置が前記データと前記識別情報の暗号化に用いるデータ暗号化鍵を生成するための手段と、

生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、

2

前記計算機のＣＰＵバスを介して前記暗号化ユニットに前記データ暗号化鍵と前記識別情報を外部から取得されることなく安全に伝えるための手段と、

自装置内に識別情報と対応して記録されているデータ暗号化鍵のうちから、データ暗号化鍵で暗号化された識別情報と該データ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化された識別情報に対応するデータ暗号化鍵を求めるための手段と、

求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化されたデータを復号するための手段とを備えたことを特徴とする復号化ユニット装置。

【請求項４】前記データ暗号化鍵を求めるための手段は、自装置内に記録されている識別情報とデータ暗号化鍵の組のうちから、前記記録媒体から読み出されたデータ暗号化鍵で暗号化された識別情報を自装置内に記録されているデータ暗号化鍵で復号して得られる識別情報と、該データ暗号化鍵に対応して自装置内に記録されている識別情報とが等しくなる組を探すことにより、復号に用いるべきデータ暗号化鍵を求めるものであることを特徴とする請求項３に記載の復号化ユニット装置。

【請求項５】前記記録媒体から読み出された暗号化されたデータを復号して得られたもとのデータに所定の変換処理を施した後に、前記計算機のＣＰＵバスを介さずに外部に出力するための手段をさらに備えたことを特徴とする請求項２ないし４のいずれか１項に記載の復号化ユニット装置。

【請求項６】　暗号化ユニット装置

計算機のＣＰＵバスを介さずに入力されたデータを、所定の記録媒体に記録する前に暗号化する暗号化ユニット装置であって、

暗号化対象となるデータの識別番号と該データの暗号化に用いるデータ暗号化鍵を生成しこれらを対応付けて記録する装置から、前記計算機のＣＰＵバスを介して前記データ暗号化鍵または前記データ暗号化鍵と前記識別情報の両方を外部から取得されることなく安全に受け取るための手段と、

受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータまたは前記暗号化対象となるデータと受け取った前記識別情報の両方を暗号化するための手段とを備えたことを特徴とする暗号化ユニット装置。

【請求項７】　暗号化ユニット装置

計算機のＣＰＵバスを介さずに入力されたデータを、所定の記録媒体に記録する前に暗号化する暗号化ユニット装置であって、

暗号化対象となるデータの識別番号と該データの暗号化に用いるデータ暗号化鍵を生成しこれらを対応付けて記録し、与えられた識別情報またはデータ暗号化鍵で暗号化された識別情報をもとにして求めたデータ暗号化鍵を

用いて与えられた暗号化されたデータを復号する復号化ユニットから、前記計算機のＣＰＵバスを介して前記データ暗号化鍵または前記データ暗号化鍵と前記識別情報の両方を外部から取得されることなく安全に受け取るための手段と、

受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータまたは前記暗号化対象となるデータと受け取った前記識別情報の両方を暗号化するための手段とを備えたことを特徴とする暗号化ユニット装置。

【請求項８】計算機のＣＰＵバスに接続された暗号化ユニットと復号化ユニットを用いてＣＰＵバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化しおよび該復号化ユニットを用いて該記録媒体に記録された暗号化されたデータを復号する暗号処理システムであって、

前記復号化ユニットは、

暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するための手段と、

前記データの識別番号を生成するための手段と、

生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、

前記計算機のＣＰＵバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段と、

自ユニット内に識別情報と対応して記録されているデータ暗号化鍵のうちから、識別情報とこれに対応するデータ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた識別情報に対応するデータ暗号化鍵を求めるための手段と、

求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化されたデータを復号するための手段を備え、

前記暗号化ユニットは、

前記計算機のＣＰＵバスを介して前記データ暗号化鍵を外部から取得されることなく安全に受け取るための手段と、

受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータを暗号化するための手段とを備えたことを特徴とする暗号処理システム。

【請求項９】計算機のＣＰＵバスに接続された暗号化ユニットと復号化ユニットを用いてＣＰＵバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化しおよび該復号化ユニットを用いて該記録媒体に記録された暗号化されたデータを復号する暗号処理システムであって、

前記復号化ユニットは、

暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するための手段と、

前記データの識別番号を生成するための手段と、

生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、

前記計算機のＣＰＵバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段と、

自ユニット内に識別情報と対応して記録されているデータ暗号化鍵のうちから、データ暗号化鍵で暗号化された識別情報と該データ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化された識別情報に対応するデータ暗号化鍵を求めるための手段と、

求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化されたデータを復号するための手段を備え、

前記暗号化ユニットは、

前記計算機のＣＰＵバスを介して前記データ暗号化鍵と前記識別情報を外部から取得されることなく安全に受け取るための手段と、

受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータと受け取った前記識別情報とをそれぞれ暗号化するための手段とを備えたことを特徴とする暗号処理システム。

【請求項１０】前記伝えるための手段および前記受け取るための手段は、それぞれ、前記計算機のＣＰＵバスを介した情報のやり取りにより協調して行われる所定の鍵共有手順により所定の一時鍵を外部から取得されることなく共有するための手段を備えるとともに、

前記伝えるための手段は、生成された前記データ暗号化鍵を共有した前記一時鍵で復号して出力するための手段を備え、

前記受け取るための手段は、与えられた前記一時鍵で復号されたデータ暗号化鍵を共有した前記一時鍵で暗号化するための手段を備えたことを特徴とする請求項８または９に記載の暗号処理システム。

【請求項１１】計算機のＣＰＵバスに接続された暗号化ユニットと復号化ユニットを用いて、該ＣＰＵバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化する暗号化方法であって、

前記復号化ユニットにて、暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するとともに、該データの識別番号を生成し、これら生成されたデータ暗号化鍵と識別番号とを対応付けて自ユニット内の所定の記録領域に記録し、

前記復号化ユニットから前記計算機のＣＰＵバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝え、

前記暗号化ユニットにて、前記暗号化対象となるデータを伝えられた前記データ暗号化鍵で暗号化することを特徴とする暗号化方法。

【請求項１２】所定の記録媒体に識別情報とともに記録

された暗号化されたデータを、計算機のＣＰＵバスに接続された、識別情報とデータ暗号化鍵とを組にして記憶している復号化ユニットを用いて復号する復号化方法であって、

自ユニット内に記録されているデータ暗号化鍵のうちから、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた識別情報に対応するデータ暗号化鍵を求め、

求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化されたデータを復号することを特徴とする復号化方法。

【請求項１３】計算機のＣＰＵバスに接続された暗号化ユニットと復号化ユニットを用いて、該ＣＰＵバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化する暗号化方法であって、

前記復号化ユニットにて、暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するとともに、該データの識別番号を生成し、これら生成されたデータ暗号化鍵と識別番号とを対応付けて自ユニット内の所定の記録領域に記録し、

前記復号化ユニットから前記計算機のＣＰＵバスを介して前記暗号化ユニットに前記データ暗号化鍵と前記識別情報を外部から取得されることなく安全に伝え、

前記暗号化ユニットにて、前記暗号化対象となるデータと伝えられた前記識別情報とを、伝えられた前記データ暗号化鍵でそれぞれ暗号化することを特徴とする暗号化方法。

【請求項１４】所定の記録媒体に暗号化された識別情報とともに記録された暗号化されたデータを、計算機のＣＰＵバスに接続された、識別情報とデータ暗号化鍵とを組にして記憶している復号化ユニットを用いて復号する復号化方法であって、

自ユニット内に記録されているデータ暗号化鍵のうちから、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられたデータ暗号化鍵で暗号化された識別情報に対応するデータ暗号化鍵を求め、

求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化されたデータを復号することを特徴とする復号化方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタル化された文書、音声、画像、プログラムなどのデータをネットワークを介して通信を行うシステムあるいは前記ディジタルデータを記録保存し、読み出しするシステムのためのユニット装置、復号化ユニット装置、暗号化ユニット装置、暗号処理システム、暗号化方法及び復号化方法に関する。

【０００２】

【従来の技術】現在、計算機が広範に普及しており、種々の分野で情報を電子化して処理し、あるいは情報を電子化して記録装置に保存することが通常行われるようになっている。また、ネットワーク環境も益々整ってきており、情報を電子化して通信することも通常行われるようになってきている。さらには、文書情報だけでなく、音声や画像などのデータを電子化して扱う技術も急速に進歩してきている。

【０００３】ところで、電子化して扱う情報には、もちろん企業秘密や個人情報のように秘匿性を要する情報が含まれる。また、著作権に係る情報のように扱いに注意を要する情報も含まれる。

【０００４】そこで、情報を電子化して扱う際に、暗号化を行っておき、正当な者だけがこれを復号できるようにする技術が良く使われている。例えば、データを暗号化して記録媒体に保存し、また記録媒体から暗号化データを読み出して復号し元のデータを取り出す暗号システムでは、予め暗号化と復号に用いる秘密鍵を定めておき、この秘密鍵を用いて保存、読み出しが行われる。このシステムによれば、秘密鍵を用いることができる者だけが保存された暗号化データを復号することができ、秘密鍵が解読されない限り、秘密鍵を用いることができない第三者が暗号化されたデータを不正に解読することはできない。

【０００５】

【発明が解決しようとする課題】しかしながら、上記システムでは、もし第三者の不正な攻撃により秘密鍵が解読されると、すべての暗号化データが解読されるばかりでなく、解読により得たデータ（プレインデータ）を自由にコピーすることが可能となってしまう。

【０００６】また、秘密鍵が解読されなくても、他の暗号化システムにも同一の秘密鍵を内蔵するような場合には、暗号化データをそのままコピーすることにより、簡単に海賊版の作成ができてしまう。

【０００７】さらに、秘密鍵が暴かれたことが発覚した場合、該当する暗号化システムの秘密鍵を更新する必要があり繁雑であるだけでなく、秘密鍵の更新後には当該暴かれた秘密鍵が復号にも使用できなくなるような更新形態をとるシステムにおいては、秘密鍵の更新後は当該暴かれた秘密鍵で暗号化されていたデータを復号することができなくなり、正当な者も元の内容を得ることができなくなってしまう不具合がある。

【０００８】本発明は、上記事情を考慮してなされたものであり、第三者による不正なコピーを防止することができるユニット装置、復号化ユニット装置、暗号化ユニット装置、暗号処理システム、暗号化方法及び復号化方法を提供することを目的とする。

【０００９】また、本発明は、第三者が鍵情報を取得しあるいは暗号化データを解読することを困難にするユニ

ット装置、復号化ユニット装置、暗号化ユニット装置、暗号処理システム、暗号化方法及び復号化方法を提供することを目的とする。

【００１０】さらに、本発明は、鍵情報の更新手続きを不要とするユニット装置、復号化ユニット装置、暗号化ユニット装置、暗号処理システム、暗号化方法及び復号化方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明は、計算機のＣＰＵバスを介さずに入力したデータ（デジタル化されたデータ；例えば、文書、音声、画像、プログラムなど）を所定の記録媒体に記録する前に暗号化する装置のために、データ暗号化鍵を生成し記録する、計算機のＣＰＵバスに接続されて使用されるユニット装置であって、暗号化対象となるデータの識別番号を生成するための手段と、前記データの暗号化に用いるデータ暗号化鍵を生成するための手段と、生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、前記計算機のＣＰＵバスを介して前記暗号化する装置に前記データ暗号化鍵または前記データ暗号化鍵と前記識別情報の両方を外部から取得されることなく安全に伝えるための手段とを備えたことを特徴とする。

【００１２】本発明は、暗号化されて所定の記録媒体に記録されたデータを復号する、計算機のＣＰＵバスに接続されて使用される復号化ユニット装置であって、前記計算機のＣＰＵバスを介さずに入力されたデータを暗号化する暗号化ユニット装置が暗号化対象とするデータの識別番号を生成するための手段と、前記暗号化ユニット装置が前記データの暗号化に用いるデータ暗号化鍵を生成するための手段と、生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、前記計算機のＣＰＵバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段と、自装置内に識別情報と対応して記録されているデータ暗号化鍵のうちから、識別情報とこれに対応するデータ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた識別情報に対応するデータ暗号化鍵を求めるための手段と、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化されたデータを復号するための手段とを備えたことを特徴とする。

【００１３】本発明は、暗号化されて所定の記録媒体に記録されたデータを復号する、計算機のＣＰＵバスに接続されて使用される復号化ユニット装置であって、前記計算機のＣＰＵバスを介さずに入力されたデータを暗号化する暗号化ユニット装置が暗号化対象とするデータの識別番号を生成するための手段と、前記暗号化ユニット装置が前記データと前記識別情報の暗号化に用いるデータ暗号化鍵を生成するための手段と、生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、前記計算機のＣＰＵバスを介して前記暗号化ユニットに前記データ暗号化鍵と前記識別情報を外部から取得されることなく安全に伝えるための手段と、自装置内に識別情報と対応して記録されているデータ暗号化鍵のうちから、データ暗号化鍵で暗号化された識別情報と該データ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化された識別情報に対応するデータ暗号化鍵を求めるための手段と、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化されたデータを復号するための手段とを備えたことを特徴とする。

【００１４】好ましくは、前記データ暗号化鍵を求めるための手段は、自装置内に記録されている識別情報とデータ暗号化鍵の組のうちから、前記記録媒体から読み出されたデータ暗号化鍵で暗号化された識別情報を自装置内に記録されているデータ暗号化鍵で復号して得られる識別情報と、該データ暗号化鍵に対応して自装置内に記録されている識別情報とが等しくなる組を探すことにより、復号に用いるべきデータ暗号化鍵を求めるものである。

【００１５】好ましくは、前記記録媒体から読み出された暗号化されたデータを復号して得られたもとのデータに所定の変換処理を施した後に、前記計算機のＣＰＵバスを介さずに外部に出力するための手段をさらに備えても良い。

【００１６】本発明は、計算機のＣＰＵバスを介さずに入力されたデータを、所定の記録媒体に記録する前に暗号化する暗号化ユニット装置であって、暗号化対象となるデータの識別番号と該データの暗号化に用いるデータ暗号化鍵を生成しこれらを対応付けて記録する装置から、前記計算機のＣＰＵバスを介して前記データ暗号化鍵または前記データ暗号化鍵と前記識別情報の両方を外部から取得されることなく安全に受け取るための手段と、受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータまたは前記暗号化対象となるデータと受け取った前記識別情報の両方を暗号化するための手段とを備えたことを特徴とする。

【００１７】本発明は、計算機のＣＰＵバスを介さずに入力されたデータを、所定の記録媒体に記録する前に暗号化する暗号化ユニット装置であって、暗号化対象となるデータの識別番号と該データの暗号化に用いるデータ暗号化鍵を生成しこれらを対応付けて記録し、与えられた識別情報またはデータ暗号化鍵で暗号化された識別情報をもとにして求めたデータ暗号化鍵を用いて与えられた暗号化されたデータを復号する復号化ユニットから、前記計算機のＣＰＵバスを介して前記データ暗号化鍵または前記データ暗号化鍵と前記識別情報の両方を外部から取得されることなく安全に受け取るための手段と、受

け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータまたは前記暗号化対象となるデータと受け取った前記識別情報の両方を暗号化するための手段とを備えたことを特徴とする。

【００１８】本発明は、計算機のＣＰＵバスに接続された暗号化ユニットと復号化ユニットを用いてＣＰＵバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化しおよび該復号化ユニットを用いて該記録媒体に記録された暗号化されたデータを復号する暗号処理システムであって、前記復号化ユニットは、暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するための手段と、前記データの識別番号を生成するための手段と、生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、前記計算機のＣＰＵバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段と、自ユニット内に識別情報と対応して記録されているデータ暗号化鍵のうちから、識別情報とこれに対応するデータ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた識別情報に対応するデータ暗号化鍵を求めるための手段と、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化されたデータを復号するための手段を備え、前記暗号化ユニットは、前記計算機のＣＰＵバスを介して前記データ暗号化鍵を外部から取得されることなく安全に受け取るための手段と、受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータを暗号化するための手段とを備えたことを特徴とする。

【００１９】好ましくは、前記記録媒体から読み出された暗号化されたデータを復号して得られたもとのデータに所定の変換処理を施した後に、前記計算機のＣＰＵバスを介さずに外部に出力するための手段をさらに備えても良い。

【００２０】本発明は、計算機のＣＰＵバスに接続された暗号化ユニットと復号化ユニットを用いてＣＰＵバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化しおよび該復号化ユニットを用いて該記録媒体に記録された暗号化されたデータを復号する暗号処理システムであって、前記復号化ユニットは、暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するための手段と、前記データの識別番号を生成するための手段と、生成されたデータ暗号化鍵と識別番号とを対応付けて記録するための手段と、前記計算機のＣＰＵバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段と、自ユニット内に識別情報と対応して記録されているデータ暗号化鍵のうちから、データ暗号化鍵で暗号化された識別情報と該データ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化された識別情報に対応するデータ暗号化鍵を求めるための手段と、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化されたデータを復号するための手段を備え、前記暗号化ユニットは、前記計算機のＣＰＵバスを介して前記データ暗号化鍵と前記識別情報を外部から取得されることなく安全に受け取るための手段と、受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータと受け取った前記識別情報とをそれぞれ暗号化するための手段とを備えたことを特徴とする。

【００２１】好ましくは、前記データ暗号化鍵を求めるための手段は、自ユニット内に記録されている識別情報とデータ暗号化鍵の組のうちから、前記記録媒体から読み出されたデータ暗号化鍵で暗号化された識別情報を自ユニット内に記録されているデータ暗号化鍵で復号して得られる識別情報と、該データ暗号化鍵に対応して自ユニット内に記録されている識別情報とが等しくなる組を探すことにより、復号に用いるべきデータ暗号化鍵を求めるものである。

【００２２】好ましくは、前記記録媒体から読み出された暗号化されたデータを復号して得られたもとのデータに所定の変換処理を施した後に、前記計算機のＣＰＵバスを介さずに外部に出力するための手段をさらに備えても良い。

【００２３】好ましくは、前記伝えるための手段および前記受け取るための手段は、それぞれ、前記計算機のＣＰＵバスを介した情報のやり取りにより協調して行われる所定の鍵共有手順により所定の一時鍵を外部から取得されることなく共有するための手段を備えるとともに、前記伝えるための手段は、生成された前記データ暗号化鍵を共有した前記一時鍵で復号して出力するための手段を備え、前記受け取るための手段は、与えられた前記一時鍵で復号されたデータ暗号化鍵を共有した前記一時鍵で暗号化するための手段を備えても良い。

【００２４】本発明は、計算機のＣＰＵバスに接続された暗号化ユニットと復号化ユニットを用いて、該ＣＰＵバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化する暗号化方法であって、前記復号化ユニットにて、暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するとともに、該データの識別番号を生成し、これら生成されたデータ暗号化鍵と識別番号とを対応付けて自ユニット内の所定の記録領域に記録し、前記復号化ユニットから前記計算機のＣＰＵバスを介して前記暗号化ユニットに前記データ暗号化鍵を外部から取得されることなく安全に伝え、前記暗号化ユニットにて、前記暗号化対象となるデータを伝えられた前記データ暗号化鍵で暗号化することを特徴とする。

11

【００２５】本発明は、所定の記録媒体に識別情報とともに記録された暗号化されたデータを、計算機のＣＰＵバスに接続された、識別情報とデータ暗号化鍵とを組にして記憶している復号化ユニットを用いて復号する復号化方法であって、自ユニット内に記録されているデータ暗号化鍵のうちから、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた識別情報に対応するデータ暗号化鍵を求め、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化されたデータを復号することを特徴とする。

【００２６】本発明は、計算機のＣＰＵバスに接続された暗号化ユニットと復号化ユニットを用いて、該ＣＰＵバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化する暗号化方法であって、前記復号化ユニットにて、暗号化対象となるデータの暗号化に用いるデータ暗号化鍵を生成するとともに、該データの識別番号を生成し、これら生成されたデータ暗号化鍵と識別番号とを対応付けて自ユニット内の所定の記録領域に記録し、前記復号化ユニットから前記計算機のＣＰＵバスを介して前記暗号化ユニットに前記データ暗号化鍵と前記識別情報を外部から取得されることなく安全に伝え、前記暗号化ユニットにて、前記暗号化対象となるデータと伝えられた前記識別情報とを、伝えられた前記データ暗号化鍵でそれぞれ暗号化することを特徴とする。

【００２７】本発明は、所定の記録媒体に暗号化された識別情報とともに記録された暗号化されたデータを、計算機のＣＰＵバスに接続された、識別情報とデータ暗号化鍵とを組にして記憶している復号化ユニットを用いて復号する復号化方法であって、自ユニット内に記録されているデータ暗号化鍵のうちから、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられたデータ暗号化鍵で暗号化された識別情報に対応するデータ暗号化鍵を求め、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記ＣＰＵバスを介して与えられた暗号化されたデータを復号することを特徴とする。

【００２８】本発明によれば、データを暗号化した暗号鍵をデータに付与した識別情報に対応して復号化ユニット内にデータベースとして記録しておくことにより、データを暗号化した計算機（あるいはデータの暗号化に用いた復号化ユニットそのものを組み込んだ計算機）でなければ復号を行うことができない。したがって、記録媒体の複製を作って頒布しても他の計算機では復号することができない。

【００２９】また、本発明によれば、データを暗号化するためのデータ暗号化鍵を、例えば共有化した一時鍵あるいはマスター鍵の鍵束の中の何れかを用いて暗号化するなどして、復号化ユニットと暗号化ユニットとの間で

12

ＣＰＵバスを介して共有するため、ＣＰＵバスからこれらの情報を記録することは無意味である。

【００３０】また、本発明によれば、データを暗号化するデータ暗号化鍵自体も、またデータ暗号化鍵を共有化するために用いる一時鍵も、毎回変わるため、第３者にとり暗号を解読することは極めて困難である。

【００３１】したがって、本発明によれば、第３者による不正なコピーを防止することが可能となる。また、本発明によれば、鍵情報の更新手続きが不要となる。

【００３２】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。本実施形態では、データを暗号化して記録媒体に記録し、また記録媒体から暗号化データを読み出し復号するシステムを例にとって説明する。

【００３３】本実施形態では、暗号化の操作をＥｙ（ｘ）と表す。ここで、ｘは暗号化の対象となるデータであり、ｙは暗号化に用いる暗号鍵である。また、復号化の操作をＤｙ（ｚ）と表す。ここで、ｚは復号化の対象となるデータであり、ｙは復号化に用いる復号鍵である。

【００３４】本実施形態では、あるデータをまず復号化し、その後、復号化されたデータを暗号化してもとのデータに戻すことがある。これは、暗号の性質上、データの復号化に暗号化と同等の作用があることに基づいている。つまり、復号化したデータをもとに戻すためには復号化に用いた鍵がわからなければならず、鍵が判れば復号化したデータを暗号化することにより最初に復号化したデータが得られる。この操作は、暗号鍵をｘとしデータをｙとすれば、

Ｅｘ（Ｄｘ（ｙ））＝ｙ

で表される。

【００３５】本実施形態に係るシステムは、パーソナル・コンピュータなどの計算機（以下、ＰＣ）内に備えられたＣＰＵ（図示せず）のＣＰＵバスに接続され、全体的な処理の流れの制御はプログラムで実現される。本実施形態では、データの入出力はＣＰＵバス以外の例えばＩ／Ｏポート等を通じて行われるが、ディスクドライブ装置（図示せず）とユニットとの間、ユニットとユニットとの間でのデータ転送には、ＣＰＵバスが用いられる。従って、ＣＰＵバス上を流れるデータには、暗号化（あるいは暗号化に先だって行う復号化）を施している。

【００３６】本実施形態は、概略的には、一纏まりのデータを暗号化する際に、データの暗号化に用いるデータ暗号化鍵Ｓｋ１と識別情報ＩＤの対を生成し、この対をデータベースに記録しておくとともに、記録媒体にはＩＤの情報とＳｋ１で暗号化したデータを記録し、再生時には記録媒体から読み出したＩＤの情報をもとにデータベースからＳｋ１を求め、Ｓｋ１を復号鍵として記録媒体に記録された暗号化データを復号するものである。

【００３７】第１，３の実施形態ではＩＤを暗号化せずに記録媒体に記録する例を、第２，４の実施形態ではＩＤをデータ暗号化鍵で暗号化して記録する例を示す。第１，３の実施形態では、データを暗号化した暗号鍵の検索を容易にし、復号時間を短縮することが可能となる。第２，４の実施形態ではＩＤを暗号化して記録媒体に記録することにより、暗号化されたデータをより厳密に第３者から守ることが可能となる。

【００３８】また、第１，２の実施形態ではＣＰＵを介したユニット間で鍵を共有する１つの例を、第３，４の実施形態ではＣＰＵを介したユニット間で鍵を共有する他の１つの例を示す。

【００３９】（第１の実施形態）図１は、本発明の第１の実施形態に係るシステムの構成を示すブロック図である。なお、図１の鍵共有回路３０ａ，３０ｂの内部構成の一例を図２に示す。また、図３に本システムの暗号化の際の手順を、図４に鍵共有手順の一例を、図５に本システムの復号の際の手順をそれぞれ示す。

【００４０】図１に示すように、本実施形態に係るシステムは、暗号化ユニット１１８と復号化ユニット１２１を備えている。また、暗号化ユニット１１８と復号化ユニット１２１は、ＰＣのＣＰＵバス１２０に接続されている。

【００４１】また、ＣＰＵバス１２０にはディスクドライブ装置（図示せず）が接続されており、ディスクドライブ装置により記録媒体１１７への読み書きが行われる。図１に示すように、暗号化ユニット１１８は、鍵共有回路３０ｂ、暗号化回路３４，１０５ｃを備えている。暗号化ユニット１１８は、独立した１つのＩＣチップとして形成されるものとする。

【００４２】復号化ユニット１２１は、データ暗号鍵生成回路１０７、ＩＤ生成回路１０８、復号化回路３２，１０６ｃ、ＩＤ／鍵情報記憶回路１０９を備えている。復号化ユニット１２１は、独立した１つのＩＣチップとして形成されるものとする。

【００４３】なお、全体の制御は図示しない制御部が司るものとする。制御部は例えばプログラムを当該ＰＣのＣＰＵで実行することにより実現することができる。データＤａｔａは、暗号化して記録する対象となる入力データであり、例えばＰＣのＩ／Ｏポートから入力される映像、音声、テキストなどのマルチメディア・データである。

【００４４】ＩＤは、本実施形態では、一纏まりのデータ毎（例えばタイトル毎）に与えられる識別番号である。なお、ＩＤは、ディスク毎に与えるようにしても良いし、ディスクの片面毎あるいは複数のディスクからなる組毎に与えるようにしても良いし、上記の一纏まりのデータをさらに細分化した部分毎（例えばチャプター毎あるいは曲毎など）に与えるようにしても良い。

【００４５】Ｓｋ１は、データの暗号化および復号に用いるデータ暗号鍵（共通鍵暗号方式における共通鍵）であり、ＩＤと対で生成される。Ｓｋｔは、ＣＰＵバス１２０上に情報を流す際に、該情報を復号（暗号化に先だって行う復号）するための、その都度変化する一時鍵（共通鍵暗号方式における共通鍵）である。

【００４６】ＩＤ生成回路１０８は、ＩＤ番号を生成する。ＩＤ番号は、１から順番に発番するようにしても良いが、好ましくはランダムに発番する方が良い。後者の場合、生成されるＩＤが全て異なるようにするために、例えばＩＤ生成回路１０８を乱数発生器を用いて構成する方法が考えられる。なお、重複発番する可能性のある乱数等を用いる場合には、生成したＩＤが既発番のものと同じであるかどうかチェックし、重複して発番されたことが分かったならば、そのＩＤは破棄し、別のＩＤを生成し直すようにすると好ましい。

【００４７】データ暗号鍵生成回路１０７は、ＩＤと対になるデータ暗号鍵Ｓｋ１を生成する。データ暗号鍵生成回路１０７は、例えば鍵長分の乱数発生器で構成しても良い。また、乱数を発生するにあたって、例えば時計（図示せず）からの時間情報を用いるようにしても良い。なお、全てのビットが０や１になる可能性のある乱数で鍵を生成する場合は、全てのビットが０や１になることがないようにチェック処理等をする必要がある。

【００４８】ＩＤ／鍵情報記憶回路１０９は、対になるＩＤとＳｋ１とを対応づけて記憶するためのものでる。例えば、ＩＤとＳｋ１をデータベース化して保管しておく。鍵共有回路３０ａ，３０ｂは、少なくとも論理的に同一の構成を有し、後述する手順により相互に情報の受け渡しをして同一の一時鍵（バス鍵）Ｓｋｔを生成し共有する。復号化ユニット１２１と暗号化ユニット１１８は、鍵共有回路３０ａ，３０ｂを用いて、同一の一時鍵Ｓｋｔを外部から知得されることなく安全に共有する。鍵共有回路３０ａ，３０ｂは外部からその内部の論理が解析されないようにＩＣチップ内に作り込むものとする。

【００４９】記録媒体１１７は、暗号化されたＩ／Ｏポートからの入力データを記録するためのものであり、例えばハードディスク、ＭＯ、ＦＤ、１回書き込み可能なＣＤ、ＤＶＤ－ＲＡＭなどを用いることが考えられる。

【００５０】なお、ディスクドライブ装置内には、記録の際に変調、誤り訂正回路を行い、再生の際に復調、誤り訂正回路を行う変復調／誤り訂正回路が内蔵される場合がある。

【００５１】また、本実施形態では、復号化ユニット１２１にはディジタルデータＤａｔａをアナログデータに変換するＤ／Ａ変換回路が備えられ、復号化ユニット１２１からはアナログに変換されらデータが出力されるものとする。また、ディジタルデータＤａｔａが復号すべきものである場合にはこれを復号する復号回路をＤ／Ａ変換回路の前に設けるものとする。例えばディジタルデ

ータＤａｔａがＭＰＥＧ方式で圧縮された画像データである場合に、ＭＰＥＧ復号回路を設けるものとする。また、種々の方式で圧縮等されたデータあるいは復号の必要ないデータのいずれも出力できるように、複数種類の復号回路を設け、これを適宜切替て使用し、あるいはこれらを使用しないように構成することも可能である。なお、復号化ユニット１２１からの出力は例えば画像としてディスプレイなどに表示される。

【００５２】最初に、図１～図４を参照しながら、暗号化の際の手順について説明する。なお、図４におけるＣＰＵはプログラムで実現した場合の制御部に相当し、ここではＣＰＵすなわち制御部が手順の仲介を行っていることを示している。なお、制御部の仲介なしにユニット間で直接情報のやり取りを行うようにしても構わない。

【００５３】まず、記録媒体１１７がリムーバブルな媒体である場合には、これをディスクドライブ装置（図示せず）にセットしておく。ステップＳ１１では、復号化ユニット１２１にて、ＩＤ生成回路１０８により入力データに対するＩＤを生成する。また、データ暗号鍵生成回路１０７により入力データを暗号化するための暗号鍵Ｓｋ１を生成する。そして、生成されたＩＤとＳｋ１とを対応付けて復号化ユニット１２１内の記憶領域１０９に記録しておく。また、生成されたＩＤを記録媒体１１７に記録する。

【００５４】なお、ＩＤは、復号化ユニット１２１からＣＰＵバスを介して直接、ディスクドライブ装置に与えても良いし、復号化ユニット１２１からＣＰＵバスを介して暗号化ユニット１１８に与え、暗号化ユニット１１８からＣＰＵバスを介してディスクドライブ装置に与えるようにしても良い。

【００５５】ステップＳ１２では、復号化ユニット１２１と暗号化ユニット１１８との間で鍵共有手順により一時鍵Ｓｋｔを共有する。ここでは、「日経エレクトロニクス　Ｎｏ．６７６　ｐｐ．１３－１４　１９９６．１１．１８」に開示された技術を応用するものとする。

【００５６】まず、本実施形態における鍵共有手順に用いる図２に示される鍵共有回路３０ａ，３０ｂの構成について説明する。鍵共有回路３０ａは、チャレンジ鍵生成回路３１ａ、認証鍵生成回路３３ａ、比較回路３５ａ、バス鍵生成回路３７ａを備えている。また、鍵共有回路３０ｂは、チャレンジ鍵生成回路３１ｂ、認証鍵生成回路３３ｂ、比較回路３５ｂ、バス鍵生成回路３７ｂを備えている。

【００５７】チャレンジ鍵生成回路３１ａ，３１ｂは、例えば乱数生成アルゴリズムを用いて、生成の都度変化するチャレンジ鍵を生成する。認証鍵生成回路３３ａ，３３ｂは、例えば一方向性関数を用いて、チャレンジ鍵から認証鍵を生成する。

【００５８】比較回路３５ａ，３５ｂは、２つの認証鍵が一致するか否か比較する。バス鍵生成回路３７ａ，３７ｂは、例えば一方向性関数を利用して、２つの認証鍵からバス鍵、すなわち一時鍵を生成する。

【００５９】認証鍵生成回路３３ａと認証鍵生成回路３３ｂは、例えば同一のアルゴリズムを用いることにより、同一のチャレンジ鍵に対して同一の認証鍵を生成するものとする。

【００６０】バス鍵生成回路３７ａとバス鍵生成回路３７ｂは、例えば同一のアルゴリズムを用いることにより、同一の２つの認証鍵から同一のバス鍵を生成するものとする。

【００６１】次に、図２、図４を参照しながら、鍵共有手順について説明する。まず、鍵共有手順のフェイズ１では、復号化ユニット１２１にて、チャレンジ鍵生成回路３１ａによりチャレンジ鍵（Ｃｈａｌｌｅｎｇｅ　Ｋｅｙ）１を生成し、これを暗号化ユニット１１８にも伝える。次に、復号化ユニット１２１の認証鍵生成回路３３ａと暗号化ユニット１１８の認証鍵生成回路３３ｂのそれぞれにて、チャレンジ鍵１をもとに認証鍵１（Ｋｅｙ１）を生成し、また暗号化ユニット１１８から復号化ユニット１２１へ生成した認証鍵１を転送する。そして、復号化ユニット１２１にて、比較回路３５ａにより、復号化ユニット１２１と暗号化ユニット１１８のそれぞれで生成された２つの認証鍵１を比較する。もし一致すれば次のフェイズ２に移行する。もし一致しなければ異常終了となる。

【００６２】次に、フェイズ２では、暗号化ユニット１１８にて、チャレンジ鍵生成回路３１ｂによりチャレンジ鍵（Ｃｈａｌｌｅｎｇｅ　Ｋｅｙ）２を生成し、これを復号化ユニット１２１にも伝える。次に、暗号化ユニット１１８の認証鍵生成回路３３ｂと復号化ユニット１２１の認証鍵生成回路３３ａのそれぞれにて、チャレンジ鍵２をもとに認証鍵２（Ｋｅｙ２）を生成し、また復号化ユニット１２１から暗号化ユニット１１８へ生成した認証鍵２を転送する。そして、暗号化ユニット１１８にて、比較回路３５ｂにより、暗号化ユニット１１８と復号化ユニット１２１のそれぞれで生成された２つの認証鍵２を比較する。もし一致すれば次のフェイズ３に移行する。もし一致しなければ異常終了となる。

【００６３】そして、フェイズ３では、復号化ユニット１２１のバス鍵生成回路３７ａと暗号化ユニット１１８のバス鍵生成回路３７ｂのそれぞれにて、認証鍵１および認証鍵２をもとにバス鍵（ＢＵＳ　Ｋｅｙ）すなわち一時鍵Ｓｋｔを生成する。

【００６４】これによって、復号化ユニット１２１と暗号化ユニット１１８との間で安全に一時鍵Ｓｋｔが共有化される。ステップＳ１３では、復号化ユニット１２１から暗号化ユニット１１８へ、共有化した一時鍵Ｓｋｔを用いてデータ暗号鍵Ｓｋ１を伝える。すなわち、まず、復号化ユニット１２１にて、復号化回路３２によりＳｋｔでＳｋ１を復号して、ＤＳｋｔ（Ｓｋ１）を得

る。次に、復号化ユニット１２１から暗号化ユニット１１８へ、ＤＳｋｔ（Ｓｋ1）を送る。そして、暗号化ユニット１１８にて、暗号化回路３４により、ＳｋｔでＤＳｋｔ（Ｓｋ１）を暗号化して、Ｓｋ１を得る。

【００６５】ステップＳ１４では、暗号化ユニット１１８にて、暗号化回路１０５ａにより、Ｓｋ１を暗号鍵として用いて入力データＤａｔａを暗号化して、ＥＳｋ１（Ｄａｔａ）を得る。

【００６６】ステップＳ１５では、ＥＳｋ１（Ｄａｔａ）を記録媒体１１７に記録する。なお、１つの記録媒体に複数のＩＤが格納される場合、ＩＤとＥＳｋ１（Ｄａｔａ）とを対応付けて格納する。

【００６７】次に、図１、図５を参照しながら、復号の際の手順について説明する。まず、記録媒体１１７がリムーバブルな媒体である場合には、これをディスクドライブ装置（図示せず）にセットしておく。

【００６８】ステップＳ２１では、記録媒体１１７に記録されたＩＤを復号化ユニット１２１へ送る。ステップＳ２２では、復号化ユニット１２１にて、送られたＩＤをもとに、記録領域１０９から、対応するＳｋ１を検索して取り出し、復号化回路１０６ｅに与える。

【００６９】ステップＳ２３では、記録媒体１１７に記録されたＥＳｋ１（Ｄａｔａ）を復号化ユニット１２１へ送る。ステップＳ２４では、復号化ユニット１２１にて、復号化回路１０６ｅにより、Ｓｋ１を復号鍵としてＥＳｋ１（Ｄａｔａ）を復号し、もとの入力データ（Ｄａｔａ）を得る。

【００７０】なお、復号対象となるデータの暗号化に用いた復号化ユニットと当該復号化ユニット１２１とが相違するものである場合、すなわち記録媒体１１７に暗号化データを記録したＰＣと当該ＰＣが相違するものである場合、復号化ユニット１２１内に対応するＩＤとＳｋ１の組が登録されていないので、上記のステップＳ２２にて対応するＳｋ１を検索して取り出すことに成功せず、結局、対象となる暗号化データを復号することはできない。言い換えると、本実施形態では、記録媒体１１７に暗号化データを記録したＰＣにおいてのみ復号を行うことができる。

【００７１】本実施形態で示した手順は一例であり種々変形することが可能である。例えば、図３において、ステップＳ１２の一時鍵の共有は最初に行っても良い。また、ステップＳ１２のＩＤの生成、データベースへの登録、記録媒体への記録は、それぞれどのようなタイミングで行っても良い。また、暗号化ユニット内にバッファがあればデータはどのようなタイミングで読み込んでも良い。また、すべてのデータを暗号化してから記録媒体に記録しても良いが、所定の単位ごとに暗号化と記録（あるいは読み込みと暗号化と記録）を繰り返し行っても良い。

【００７２】また、例えば図５において、復号化ユニット内にバッファがあれば暗号化データはどのようなタイミングで読み込んでも良い。また、すべてのデータを復号してから出力しても良いが、所定の単位ごとに復号と出力（あるいは読み込みと復号と出力）を繰り返し行っても良い。

【００７３】上記の暗号化回路と復号化回路で用いる暗号化方式は、すべての部分で同じものを用いても良いし、対になる暗号化回路と復号化回路の組ごとに、用いる暗号化方式を適宜決めても良い（すべて異なるようにすることも可能である）。

【００７４】また、上記では暗号化回路や復号化回路は独立した回路として示したが、暗号化回路や復号化回路は暗号化方式が同じであればユニット内において１つまたは複数のもので兼用するように構成しても構わない。すなわち、復号化ユニット１２１の復号化回路２１と暗号化ユニット１１８の暗号化回路３２の暗号化方式と、復号化ユニット１２１の復号化回路１０６ｃと暗号化ユニット１１８の暗号化回路１０５ｃの暗号化方式が同じである場合に、復号化ユニット１２１において復号化回路２１と復号化回路１０６ｃを１つの回路で構成しても良いし、同様に暗号化ユニット１１８において暗号化回路３２と暗号化回路１０５ｃを１つの回路で構成しても良い。

【００７５】本実施形態では、暗号化ユニットはＰＣ内に例えば暗号化ボードとして組み込まれＣＰＵバスに接続されるものであったが、暗号化ユニットはディスクドライブ装置内に内蔵されることもある。

【００７６】なお、図１の構成において、復号化ユニット１２１を２つのＩＣチップに分離して構成することも可能である。例えば、復号化ユニット１２１から復号化回路１０６ｃを分離し、これに鍵共有回路３０ａと同じものと暗号化回路を付加してＩＣチップ化し（これを第３ユニットとする）、復号の際には復号化ユニット１２１と第３ユニットとの間で鍵共有回路により一時鍵を共有化した後、復号化ユニット１２１から第３ユニットへＣＰＵバス１２０を介して一時鍵で復号化したデータ暗号化鍵を送り、第３ユニットにてこれを一時鍵で暗号化してデータ暗号化鍵を得るようにしても良い。なお、この場合、復号化ユニット１２１に新たに復号化回路を付け加えても良いが、すでに存在する復号化回路を兼用しても良い。

【００７７】（第２の実施形態）図６は、本発明の第２の実施形態に係るシステムの構成を示すブロック図である。なお、図６の鍵共有回路３０ａ，３０ｂの内部構成の一例を図２に示す。また、図７に本システムの暗号化の際の手順を、図４に鍵共有手順の一例を、図８に本システムの復号の際の手順をそれぞれ示す。

【００７８】本実施形態は、基本的には第１の実施形態と同様の構成を有するものであり、以下では、主に相違する点について説明する。まず、暗号化ユニット１１８

は、図１の構成と同様であるが、復号化ユニット１２１から渡されたＤＳｋｔ（ＩＤ）を、暗号化回路３２により一時鍵で復号する点、復号されたＩＤを暗号化回路１０５ｃによりＳｋ１で暗号化する点が相違する。

【００７９】また、復号化ユニット１２１は、図１の構成に加えて、与えられたＥＳｋ１（ＩＤ）からＳｋ１を得るための復号化回路１０６ｄとＩＤ判定回路１１０が付加されており、また生成したＩＤをも復号化回路３２により一時鍵Ｓｋｔで復号化して暗号化ユニット１１８に送る点が相違する。

【００８０】次に、図６、図７、図２、図４を参照しながら、暗号化の際の手順について説明する。ステップＳ３１では、復号化ユニット１２１にて、ＩＤ生成回路１０８により入力データに対するＩＤを生成する。また、データ暗号鍵生成回路１０７により入力データを暗号化するための暗号鍵Ｓｋ１を生成する。そして、生成されたＩＤとＳｋ１とを対応付けて復号化ユニット１２１内の記憶領域１０９に記録しておく。

【００８１】ステップＳ３２では、ステップＳ１２と同様にして、復号化ユニット１２１と暗号化ユニット１１８との間で鍵共有手順により一時鍵Ｓｋｔを共有する。ステップＳ３３では、復号化ユニット１２１から暗号化ユニット１１８へ、共有化した一時鍵Ｓｋｔを用いてデータ暗号鍵Ｓｋ１とＩＤを伝える。

【００８２】すなわち、データ暗号鍵Ｓｋ１については、まず、復号化ユニット１２１にて、復号化回路３２によりＳｋｔでＳｋ１を復号して、ＤＳｋｔ（Ｓｋ１）を得る。次に、復号化ユニット１２１から暗号化ユニット１１８へ、ＤＳｋｔ（Ｓｋ１）を送る。そして、暗号化ユニット１１８にて、暗号化回路３４により、ＳｋｔでＤＳｋｔ（Ｓｋ１）を暗号化して、Ｓｋ１を得る。

【００８３】また、ＩＤについては上記と同様に、復号化ユニット１２１にて、復号化回路３２によりＳｋｔでＩＤを復号して、ＤＳｋｔ（ＩＤ）を得る。次に、復号化ユニット１２１から暗号化ユニット１１８へ、ＤＳｋｔ（ＩＤ）を送る。そして、暗号化ユニット１１８にて、暗号化回路３４により、ＳｋｔでＤＳｋｔ（ＩＤ）を暗号化して、ＩＤを得る。

【００８４】ステップＳ３４では、暗号化ユニット１１８にて、暗号化回路１０５ｃにより、Ｓｋ１を暗号鍵として用いてＩＤを暗号化して、ＥＳｋ１（ＩＤ）を得る。そして、ＥＳｋ１（ＩＤ）を記録媒体１１７に記録する。

【００８５】ステップＳ３５では、暗号化ユニット１１８にて、暗号化回路１０５ｃにより、Ｓｋ１を暗号鍵として用いて入力データＤａｔａを暗号化して、ＥＳｋ１（Ｄａｔａ）を得る。そして、ＥＳｋ１（Ｄａｔａ）を記録媒体１１７に記録する。

【００８６】なお、１つの記録媒体に複数のＥＳｋ１（ＩＤ）が格納される場合、ＥＳｋ１（ＩＤ）とＥＳｋ１（Ｄａｔａ）とを対応付けて格納する。次に、図６、図８を参照しながら、復号の際の手順について説明する。

【００８７】まず、記録媒体１１７がリムーバブルな媒体である場合には、これをディスクドライブ装置（図示せず）にセットして、ディスクドライブ装置は、記録媒体１１７に記録されたＥＳｋ１'（ＩＤ）を復号化ユニット１２１へ送る。

【００８８】ステップＳ４２では、復号化ユニット１２１にて、送られたＥＳｋ１（ＩＤ）をもとに記録領域１０９から対応するＳｋ１を求める。すなわち、まず、復号化回路１０６ｄにより、記録領域１０９に記録されている１つの暗号鍵を使って、ＥＳｋ１（ＩＤ）を復号し、この結果をＩＤ候補とし、ＩＤ判定回路１１０に与える。また、この１つの暗号鍵に対応して記録領域１０９に記録されているＩＤをＩＤ判定回路１１０に与える。そして、ＩＤ判定回路１１０により、両者を比較して、一致しなければ、記録領域１０９に記憶されている他の暗号鍵を使って同様の手順を行う。そして、ＩＤ判定回路１１０により、両者を比較して、一致すれば、そのＳｋ１とＩＤの組が求めるべきものであるので、記録領域１０９からあるいは復号化回路１０６からそのＳｋ１を復号化回路１０６ｄに与える。

【００８９】ステップＳ４３では、記録媒体１１７に記録されたＥＳｋ１（Ｄａｔａ）を復号化ユニット１２１へ送る。ステップＳ４４では、復号化ユニット１２１にて、復号化回路１０６ｃにより、Ｓｋ１を復号鍵としてＥＳｋ１（Ｄａｔａ）を復号し、もとの入力データを得る。

【００９０】本実施形態で示した手順は一例であり種々変形することが可能である。例えば、図７において、ステップＳ３２の一時鍵の共有は最初に行っても良い。また、ステップＳ３１のＩＤの生成、Ｓｋ１の生成は、ステップＳ３２の後に行っても良い。また、ステップＳ３１のデータベースへの登録は、どのようなタイミングで行っても良い。また、ステップＳ３３において、ＩＤとＳｋ１のいずれを先に共有しても構わない。また、暗号化ユニット内にバッファがあればデータはどのようなタイミングで読み込んでも良い。また、すべてのデータを暗号化してから記録媒体に記録しても良いが、所定の単位ごとに暗号化と記録（あるいは読み込みと暗号化と記録）を繰り返し行っても良い。

【００９１】また、例えば図８において、復号化ユニット内にバッファがあれば暗号化データはどのようなタイミングで読み込んでも良い。また、すべてのデータを復号してから出力しても良いが、所定の単位ごとに復号と出力（あるいは読み込みと復号と出力）を繰り返し行っても良い。

【００９２】なお、第１の実施形態と同様に、暗号化回路や復号化回路は暗号化方式が同じであればユニット内

において１つまたは複数のもので兼用するように構成しても構わない。本実施形態では、復号化ユニット１２１において、復号化回路３２，１０６ｃ，１０６ｄを１つの回路で構成することも可能であり、また、２つの回路（例えば、復号化回路３２と、復号化回路１０６ｃ，１０６ｄに共通する回路）で構成することも可能である。

【００９３】（第３の実施形態）図９は、本発明の第３の実施形態に係るシステムの構成を示すブロック図である。図１０は、本システムの暗号化の際の手順を示すフローチャートである。図１１は、本システムの復号の際の手順を示すフローチャートである。

【００９４】図９に示すように、本実施形態に係るシステムは、暗号化ユニット１１８と復号化ユニット１２１を備えている。また、暗号化ユニット１１８と復号化ユニット１２１は、ＰＣのＣＰＵバス１２０に接続されている。

【００９５】また、ＣＰＵバス１２０にはディスクドライブ装置（図示せず）が接続されており、ディスクドライブ装置により記録媒体１１７への読み書きが行われる。図９に示すように、暗号化ユニット１１８は、暗号化回路１０５ａ～１０５ｃ、鍵判定回路２１０を備えている。暗号化ユニット１１８は、独立した１つのＩＣチップとして形成されるものとする。

【００９６】復号化ユニット１２１は、データ暗号鍵生成回路１０７、ＩＤ生成回路１０８、復号化回路１０６ａ～１０６ｃ、ＩＤ／鍵情報記憶回路１０９を備えている。復号化ユニット１２１は、独立した１つのＩＣチップとして形成されるものとする。

【００９７】復号化ユニット１２１内には、後述する複数のマスター鍵Ｍｋｓ（図中１０２ａ）が登録されている（作り込まれている）。また、暗号化ユニット１１８内には、復号化ユニット１２１と同一の複数のマスター鍵Ｍｋｓ（図中１０２ｂ）が登録されている（作り込まれている）。

【００９８】なお、万一、マスター鍵が破られたことが発覚した場合、それ以降、復号化ユニット１２１には、その破られたものを除いてマスター鍵が作り込まれる。ただし、暗号化ユニット１１８については、その破られたものを除いてマスター鍵が作り込まれても良いし、そうしなくても良い。また、破られたマスター鍵が作り込まれている復号化ユニット２０３は、その破られたものを除いてマスター鍵が作り込まれている新しいものに差し替えるのが望ましい。ただし、暗号化ユニット１１８は、破られたマスター鍵が作り込まれているものをそのまま使用しても構わない。

【００９９】なお、全体の制御は図示しない制御部が司るものとする。制御部は例えばプログラムを当該ＰＣのＣＰＵで実行することにより実現することができる。データＤａｔａは、暗号化して記録する対象となる入力データであり、例えばＰＣのＩ／Ｏポートから入力される映像、音声、テキストなどのマルチメディア・データである。

【０１００】ＩＤは、本実施形態では、一纏まりのデータ毎（例えばタイトル毎）に与えられる識別番号である。なお、ＩＤは、ディスク毎に与えるようにしても良いし、ディスクの片面毎あるいは複数のディスクからなる組毎に与えるようにしても良いし、上記の一纏まりのデータをさらに細分化した部分毎（例えばチャプター毎あるいは曲毎など）に与えるようにしても良い。

【０１０１】Ｓｋ１は、データの暗号化および復号に用いるデータ暗号鍵（共通鍵暗号方式における共通鍵）であり、ＩＤと対で生成される。Ｍｋｓ（ｓ＝１～ｎ、ｎは２以上の整数）は、マスター鍵（共通鍵暗号方式における共通鍵）の鍵束である。マスター鍵は、例えばメーカ毎に所定個数づつが割り当てられる。この場合、マスター鍵は、メーカ間で重複のないように割り当てられる。ここでは、一例として、ｓ＝１，…１０（ｓ＝１０）とする。つまり、Ｍｋ１，Ｍｋ２，…，Ｍｋ１０のマスター鍵が、暗号化ユニット１１８、復号化ユニット１２１のそれぞれに作り込まれる。

【０１０２】前述したように、マスター鍵の鍵束は、利用者が外部から取得できないように、暗号化ユニットのチップ、復号化ユニットのチップそれぞれにおいて、利用者が意図的に取り出せないようにチップ内部の秘匿された領域に記録されているものとする。

【０１０３】ＩＤ生成回路１０８は、ＩＤ番号を生成する。ＩＤ番号は、１から順番に発番するようにしても良いが、好ましくはランダムに発番する方が良い。後者の場合、生成されるＩＤが全て異なるようにするために、例えばＩＤ生成回路１０８を乱数発生器を用いて構成する方法が考えられる。なお、重複発番する可能性のある乱数等を用いる場合には、生成したＩＤが既発番のものと同じであるかどうかチェックし、重複して発番されたことが分かったならば、そのＩＤは破棄し、別のＩＤを生成し直すようにすると好ましい。

【０１０４】データ暗号鍵生成回路１０７は、ＩＤと対になるデータ暗号鍵Ｓｋ１を生成する。一時鍵生成回路１０７は、例えば鍵長分の乱数発生器で構成しても良い。また、乱数を発生するにあたって、例えば時計（図示せず）からの時間情報を用いるようにしても良い。なお、全てのビットが０や１になる可能性のある乱数で鍵を生成する場合は、全てのビットが０や１になることがないようにチェック処理等をする必要がある。

【０１０５】ＩＤ／鍵情報記憶回路１０９は、対になるＩＤとＳｋ１とを対応づけて記憶するためのものでる。例えば、ＩＤとＳｋ１をデータベース化して保管しておく。記録媒体１１７は、暗号化されたＩ／Ｏポートからの入力データを記録するためのものであり、例えばハードディスク、ＭＯ、ＦＤ、１回書き込み可能なＣＤ、ＤＶＤ－ＲＡＭなどを用いることが考えられる。

【０１０６】なお、ディスクドライブ装置内には、記録の際に変調、誤り訂正回路を行い、再生の際に復調、誤り訂正回路を行う変復調／誤り訂正回路が内蔵される場合がある。

【０１０７】また、本実施形態では、復号化ユニット１２１にてディジタルデータとしてアナログデータに変換するＤ／Ａ変換回路が備えられ、復号化ユニット１２１からはアナログに変換されらデータが出力されるものとする。また、ディジタルデータＤａｔａが復号すべきものである場合にはこれを復号する復号回路をＤ／Ａ変換回路の前に設けるものとする。例えばディジタルデータＤａｔａがＭＰＥＧ方式で圧縮された画像データである場合に、ＭＰＥＧ復号回路を設けるものとする。また、種々の方式で圧縮等されたデータあるいは復号の必要ないデータのいずれも出力できるように、複数種類の復号回路を設け、これを適宜切替て使用し、あるいはこれらを使用しないように構成することも可能である。なお、復号化ユニット１２１からの出力は例えば画像としてディスプレイなどに表示される。

【０１０８】最初に、図９、図１０を参照しながら、暗号化の際の手順について説明する。まず、記録媒体１１７がリムーバブルな媒体である場合には、これをディスクドライブ装置（図示せず）にセットしておく。

【０１０９】ステップＳ５１では、復号化ユニット１２１にて、ＩＤ生成回路１０８により入力データに対するＩＤを生成する。また、データ暗号鍵生成回路１０７により入力データを暗号化するための暗号鍵Ｓｋ１を生成する。そして、生成されたＩＤとＳｋ１とを対応付けて復号化ユニット１２１内の記憶領域１０９に記録しておく。また、生成されたＩＤを記録媒体１１７に記録する。

【０１１０】なお、ＩＤは、復号化ユニット１２１からＣＰＵバスを介して直接、ディスクドライブ装置に与えても良いし、復号化ユニット１２１からＣＰＵバスを介して暗号化ユニット１１８に与え、暗号化ユニット１１８からＣＰＵバスを介してディスクドライブ装置に与えるようにしても良い。

【０１１１】ステップＳ５２では、以下に示すような手順を用いて、復号化ユニット１２１から暗号化ユニット１１８へ、生成されたデータ暗号鍵Ｓｋ１を伝える。Ｓｋ１のプレインデータを取得されないように、Ｓｋ１は、復号化ユニット１２１内に記録されたマスター鍵Ｍｋｓ（ｓ＝１，…，ｎ）のうちのいずれか（これをＭｋｉとする）で暗号化され、ＥＭｋｉ（Ｓｋ１）としてＣＰＵバス１２０を通って暗号化ユニット１１８へ送られる。

【０１１２】ここで、もしマスター鍵が１つだけ存在するのであれば（これをＭｋ０とする）、単に復号化ユニット１２１にてＭｋ０でＳｋ１を復号し、このＥＭｋ０（Ｓｋ１）を暗号化ユニット１１８へ送り、暗号化ユニット１１８にてＭｋ０でＥＭｋ０（Ｓｋ１）を暗号化することにより、Ｓｋ１を取り出すことができるが、本実施形態では、複数のマスター鍵からなる鍵束のうちの使用したマスター鍵Ｍｋｉを直接的に指し示す識別情報は復号化ユニット１２１から暗号化ユニット１１８へ伝えないようにし、その代わりに、上記マスター鍵Ｍｋｉを特定可能とする情報を復号化ユニット１２１から復号化ユニット１２１へ送り、暗号化ユニット１１８にて、Ｓｋｔの復号に使用されたマスター鍵Ｍｋｉがｎ個のマスター鍵のうちのいずれであるかを特定するとともに、このマスター鍵の特定を通じてＳｋ１を得る。

【０１１３】以下、ステップＳ５２のより詳しい手順について説明する。まず、復号化ユニット１２１にて、復号化回路１０６ａにより、ｎ個のマスター鍵Ｍｋｓ（ｉ＝１，…，ｎ）のうちから例えばランダムあるいは順番に選んだ１つ（これをＭｋｉとする）でデータ暗号化鍵Ｓｋ１を復号して、ＤＭｋｉ（Ｓｋ１）を得る。また、復号化回路１０６ｂにより、Ｓｋ１自身を復号鍵として用いてＳｋ１を復号して、ＤＳｋ１（Ｓｋ１）を得る。そして、ＤＭｋｉ（Ｓｋ１）とＤＳｋ１（Ｓｋ１）を、ＣＰＵバス１２０を通じて暗号化ユニット１１８へ送る。

【０１１４】次に、暗号化ユニット１１８にて、まずマスター鍵を１つ選ぶ（これをＭｋｐとする）。選んだＭｋｐを復号鍵として、暗号化回路１０５ａにより、ＤＭｋｉ（Ｓｋ１）を暗号化し、

ＥＭｋｐ（ＤＭｋｉ（Ｓｋ１））＝Ｓｋａ

を得る。

【０１１５】次に、暗号化回路１０５ａの出力Ｓｋａを復号鍵として、暗号化回路１０５ｂにより、ＤＳｋ１（Ｓｋ１）を暗号化し、

ＥＳｋａ（ＤＳｋ１（Ｓｋ１））＝Ｓｋｂ

を得る。

【０１１６】次に、鍵判定回路２１０により、ＳｋａとＳｋｂとが一致するか否か調べる。ここで、復号化ユニット１２１にてＳｋ１を暗号化したマスター鍵ＭｋｉがＭｋｐであったならば、

Ｓｋａ＝ＥＭｋｐ（ＤＭｋｉ（Ｓｋ１））＝Ｓｋ１

となり、従って、

Ｓｋｂ＝ＥＳｋａ（ＤＳｋ１（Ｓｋ１））＝ＥＳｋ１（ＤＳｋ１（Ｓｋ１））＝Ｓｋ１

となり、ゆえに、

Ｓｋａ＝Ｓｋｂ＝Ｓｋ１

となる。

【０１１７】つまり、鍵判定回路２１０により、ＳｋａとＳｋｂとが一致することがわかった場合には、Ｍｋｉ＝Ｍｋｐ、かつ、Ｓｋａ＝Ｓｋｂ＝Ｓｋ１であり、この場合、鍵判定回路２１０はＳｋａ＝Ｓｋｂ＝Ｓｋ１を出力する。

【０１１８】一方、鍵判定回路２１０により、Ｓｋａと

Ｓｋｂとが一致しないことがわかった場合には、Ｍｋｉ≠Ｍｋｐであり、復号化ユニット１２１にてＳｋ１はこのＭｋｐでは暗号化されておらず、それ以外のマスター鍵で暗号化されたことが判る。この場合、鍵判定回路２１０は出力をしない（あるいは鍵判定回路２１０の出力が暗号化回路１０５ｃには伝えられない）。

【０１１９】以降は、ＳｋａとＳｋｂとが一致するまで、暗号化に用いるマスター鍵Ｍｋｐを変更して、上記の手順を繰り返す。例えば、最初にＭｋｐとしてＭｋ１を用いて上記の手順を行ってＳｋａとＳｋｂとが一致しなかった場合に、次にＭｋ２へと更新して再び上記の手順を繰り返すのである。

【０１２０】以上のような手順を用いて、復号化ユニット１２１にてどのマスター鍵を用いたのかを暗号化ユニット１１８側で特定することができるとともに、復号化ユニット１２１と暗号化ユニット１１８との間でデータ暗号化鍵Ｓｋ１を安全に共有することが可能となる。

【０１２１】ステップＳ５３では、暗号化ユニット１１８にて、暗号化回路１０５ｃにより、Ｓｋ１を暗号鍵として用いて入力データＤａｔａを暗号化して、ＥＳｋ１（Ｄａｔａ）を得る。

【０１２２】ステップＳ５４では、ＥＳｋ１（Ｄａｔａ）を記録媒体１１７に記録する。なお、１つの記録媒体に複数のＩＤが格納される場合、ＩＤとＥＳｋ１（Ｄａｔａ）とを対応付けて格納する。

【０１２３】次に、図９、図１１を参照しながら、復号の際の手順について説明する。まず、記録媒体１１７がリムーバブルな媒体である場合には、これをディスクドライブ装置（図示せず）にセットしておく。

【０１２４】ステップＳ６１では、記録媒体１１７に記録されたＩＤを復号化ユニット１２１へ送る。ステップＳ６２では、復号化ユニット１２１にて、送られたＩＤをもとに、記録領域１０９から、対応するＳｋ１を検索して取り出し、復号化回路１０６ｅに与える。

【０１２５】ステップＳ６３では、記録媒体１１７に記録されたＥＳｋ１（Ｄａｔａ）を復号化ユニット１２１へ送る。ステップＳ６４では、復号化ユニット１２１にて、復号化回路１０６ｅにより、Ｓｋ１を復号鍵としてＥＳｋ１（Ｄａｔａ）を復号し、もとの入力データ（Ｄａｔａ）を得る。

【０１２６】なお、復号対象となるデータの暗号化に用いた復号化ユニットと当該復号化ユニットｉ２１とが相違するものである場合、すなわち記録媒体１１７に暗号化データを記録したＰＣと当該ＰＣが相違するものである場合、復号化ユニット１２１内に対応するＩＤとＳｋ１の組が登録されていないので、上記のステップＳ２２にて対応するＳｋ１を検索して取り出すことに成功せず、結局、対象となる暗号化データを復号することはできない。言い換えると、本実施形態では、記録媒体１１７に暗号化データを記録したＰＣにおいてのみ復号を行うことができる。

【０１２７】本実施形態で示した手順は一例であり種々変形することが可能である。例えば、図１０において、ステップＳ５１のＩＤの生成、データベースへの登録、記録媒体への記録は、それぞれどのようなタイミングで行っても良い。また、暗号化ユニット内にバッファがあればデータはどのようなタイミングで読み込んでも良い。また、すべてのデータを暗号化してから記録媒体に記録しても良いが、所定の単位ごとに暗号化と記録（あるいは読み込みと暗号化と記録）を繰り返し行っても良い。図１１については、第１の実施形態と同様である。

【０１２８】上記の暗号化回路や復号化回路で用いる暗号化方式は、すべての部分で同じものを用いても良いし、対になる暗号化回路と復号化回路の組ごとに、用いる暗号化方式を適宜決めても良い（すべて異なるようにすることも可能である）。

【０１２９】また、上記では暗号化回路や復号化回路は独立した回路として示したが、暗号化回路や復号化回路は暗号化方式が同じであればユニット内において１つまたは複数のもので兼用するように構成しても構わない。例えば、復号化ユニット１２１において、復号化回路１０６ａ，１０６ｂ，１０６ｃを1つの回路で構成することも可能であり、また、２つの回路（例えば、復号化回路１０６ａ，１０６ｂに共用する回路と、復号化回路１０６ｃ）で構成することも可能である。また、例えば、暗号化ユニット１１８において、暗号化回路１０５ａ，１０５ｂ，１０５ｃを1つの回路で構成することも可能であり、また、２つの回路（例えば、暗号化回路１０５ａ，１０５ｂに共用する回路と、暗号化回路１０５ｃ）で構成することも可能である。

【０１３０】なお、第１の実施形態と同様に、図９の構成においても、復号化ユニット１２１を２つのＩＣチップに分離して構成することも可能である。

（第４の実施形態）図１２は、本発明の第４の実施形態に係るシステムの構成を示すブロック図である。図１３は、本システムの暗号化の際の手順を示すフローチャートである。図１４は、本システムの復号の際の手順を示すフローチャートである。

【０１３１】本実施形態は、基本的には第３の実施形態と同様の構成を有するものであり、以下では、主に相違する点について説明する。まず、暗号化ユニット１１８は、図９の構成と同様であるが、復号化ユニット１２１から渡されたＤＭｋｉ（ＩＤ）を、マスター鍵Ｍｋｉが特定された後に暗号化回路１０５ａによりこのマスター鍵Ｍｋｉで復号する点、復号されたＩＤを暗号化回路１０５ｃによりＳｋ１で暗号化する点が相違する。

【０１３２】また、復号化ユニット１２１は、図９の構成に加えて、与えられたＥＳｋ１（ＩＤ）からＳｋ１を得るための復号化回路１０６ｄとＩＤ判定回路１１０が付加されており、また生成したＩＤをも復号化回路１０

６ａによりマスター鍵Ｍｋｉで復号化して暗号化ユニット１１８に送る点が相違している。

【０１３３】次に、図１２、図１３を参照しながら、暗号化の際の手順について説明する。ステップＳ７１では、復号化ユニット１２１にて、ＩＤ生成回路１０８により入力データに対するＩＤを生成する。また、データ暗号鍵生成回路１０７により入力データを暗号化するための暗号鍵Ｓｋ１を生成する。そして、生成されたＩＤとＳｋ１とを対応付けて復号化ユニット１２１内の記憶領域１０９に記録しておく。

【０１３４】ステップＳ７２では、以下に示すような手順を用いて、復号化ユニット１２１から暗号化ユニット１１８へ、生成されたデータ暗号鍵Ｓｋ１とＩＤを伝える。まず、復号化ユニット１２１にて、復号化回路１０６ａにより、ｎ個のマスター鍵Ｍｋｓ（ｉ＝１，…，ｎ）のうちのずれか（これをＭｋｉとする）でデータ暗号化鍵Ｓｋ１を復号して、ＤＭｋｉ（Ｓｋ１）を得る。また、復号化回路１０６ｂにより、Ｓｋ１自身を復号鍵として用いてＳｋ１を復号して、ＤＳｋ１（Ｓｋ１）を得る。そして、ＤＭｋｉ（Ｓｋ１）とＤＳｋ１（Ｓｋ１）を、ＣＰＵバス１２０を通じて暗号化ユニット１１８へ送る。また、復号化回路１０６ａにより、ＩＤも同じＭｋｉで復号して、ＤＭｋｉ（ＩＤ）を求め、これもＣＰＵバス１２０を通じて暗号化ユニット１１８へ送る。

【０１３５】次に、ステップＳ５２と同様にして、暗号化ユニット１１８にて、マスター鍵Ｍｋｉを特定するとともに、データ暗号化鍵Ｓｋ１を求める。そして、暗号化回路１０５ａにより、特定したＭｋｉでＥＭｋｉ（ＩＤ）を復号して、ＩＤを得る。

【０１３６】ステップＳ７３では、暗号化ユニット１１８にて、暗号化回路１０５ｃにより、Ｓｋ１を暗号鍵として用いてＩＤを暗号化して、ＥＳｋ１（ＩＤ）を得る。そして、ＥＳｋ１（ＩＤ）を記録媒体１１７に記録する。

【０１３７】ステップＳ７４では、暗号化ユニット１１８にて、暗号化回路１０５ｃにより、Ｓｋ１を暗号鍵として用いて入力データＤａｔａを暗号化して、ＥＳｋ１（Ｄａｔａ）を得る。そして、ＥＳｋ１（Ｄａｔａ）を記録媒体１１７に記録する。

【０１３８】なお、１つの記録媒体に複数のＥＳｋ１（ＩＤ）が格納される場合、ＥＳｋ１（ＩＤ）とＥＳｋ１（Ｄａｔａ）とを対応付けて格納する。次に、図１２、図１４を参照しながら、復号の際の手順について説明する。

【０１３９】まず、記録媒体１１７がリムーバブルな媒体である場合には、これをディスクドライブ装置（図示せず）にセットしておく。ステップＳ８１では、記録媒体１１７に記録されたＥＳｋ１（ＩＤ）を復号化ユニット１２１へ送る。

【０１４０】ステップＳ８２では、復号化ユニット１２１にて、送られたＥＳｋ１（ＩＤ）をもとに記録領域１０９から対応するＳｋ１を求める。すなわち、まず、復号化回路１０６ｄにより、記録領域１０９に記録されている１つの暗号鍵を使って、ＥＳｋ１（ＩＤ）を復号し、この結果をＩＤ候補とし、ＩＤ判定回路１１０に与える。また、この１つの暗号鍵に対応して記録領域１０９に記録されているＩＤをＩＤ判定回路１１０に与える。そして、ＩＤ判定回路１１０により、両者を比較して、一致しなければ、記録領域１０９に記憶されている他の暗号鍵を使って同様の手順を行う。そして、ＩＤ判定回路１１０により、両者を比較して、一致すれば、そのＳｋ１とＩＤの組が求めるべきものであるので、記録領域１０９からあるいは復号化回路１０６からそのＳｋ１を復号化回路１０６ｄに与える。

【０１４１】ステップＳ８３では、記録媒体１１７に記録されたＥＳｋ１（Ｄａｔａ）を復号化ユニット１２１へ送る。ステップＳ８４では、復号化ユニット１２１にて、復号化回路１０６ｃにより、Ｓｋ１を復号鍵としてＥＳｋ１（Ｄａｔａ）を復号し、もとの入力データを得る。

【０１４２】本実施形態で示した手順は一例であり種々変形することが可能である。例えば、図１３において、ステップＳ７１のＩＤの生成、データベースへの登録、記録媒体への記録は、それぞれどのようなタイミングで行っても良い。また、暗号化ユニット内にバッファがあればデータはどのようなタイミングで読み込んでも良い。また、すべてのデータを暗号化してから記録媒体に記録しても良いが、所定の単位ごとに暗号化と記録（あるいは読み込みと暗号化と記録）を繰り返し行っても良い。図１１については、第２の実施形態と同様である。

【０１４３】第３の実施形態と同様に、暗号化回路や復号化回路は暗号化方式が同じであればユニット内において１つまたは複数のもので兼用するように構成しても構わない。本実施形態では、例えば、復号化ユニット１２１において、復号化回路１０６ａ，１０６ｂ，１０６ｃ，１０６ｄを１つの回路で構成することも可能であり、また、２つの回路（例えば、復号化回路１０６ａ，１０６ｂに共用する回路と、復号化回路１０６ｃ，１０６ｄに共用する回路）で構成することも可能であり、また、３つの回路で構成することも可能である。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０１４４】

【発明の効果】本発明によれば、その都度生成するデータ暗号化鍵を識別情報と対応させてユニット内に記録しておくことにより、このユニットそのものがなければ復号を行うことができず、記録媒体の複製を作っても他の計算機では復号することができない。

【０１４５】また、本発明によれば、ＣＰＵバスを流れるデータ暗号化鍵は暗号化されており、またデータ暗号化鍵自体もその都度生成されるものであるため、第３者により暗号を解読することは極めて困難である。したがって、本発明によれば、第３者による不正なコピーを防止することが可能となる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るシステムの構成を示すブロック図

【図２】図１の鍵共有回路の内部構成の一例を示す図

【図３】同実施形態における暗号化の際の手順を示すフローチャート

【図４】鍵共有手順の一例を示すフローチャート

【図５】同実施形態における復号の際の手順を示すフローチャート

【図６】本発明の第２の実施形態に係るシステムの構成を示すブロック図

【図７】同実施形態における暗号化の際の手順を示すフローチャート

【図８】同実施形態における復号の際の手順を示すフローチャート

【図９】本発明の第３の実施形態に係るシステムの構成を示すブロック図

【図１０】同実施形態における暗号化の際の手順を示すフローチャート

【図１１】同実施形態における復号の際の手順を示すフローチャート

【図１２】本発明の第４の実施形態に係るシステムの構成を示すブロック図

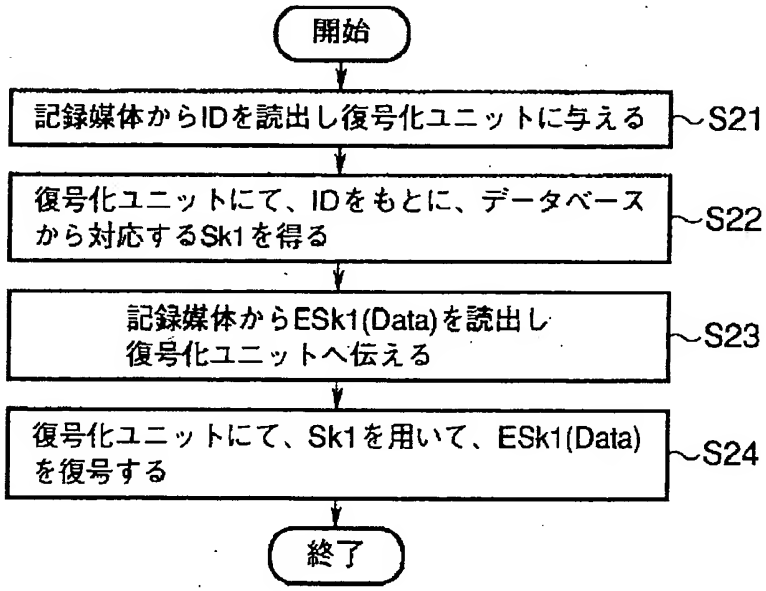
【図１３】同実施形態における暗号化の際の手順を示すフローチャート

【図１４】同実施形態における復号の際の手順を示すフローチャート

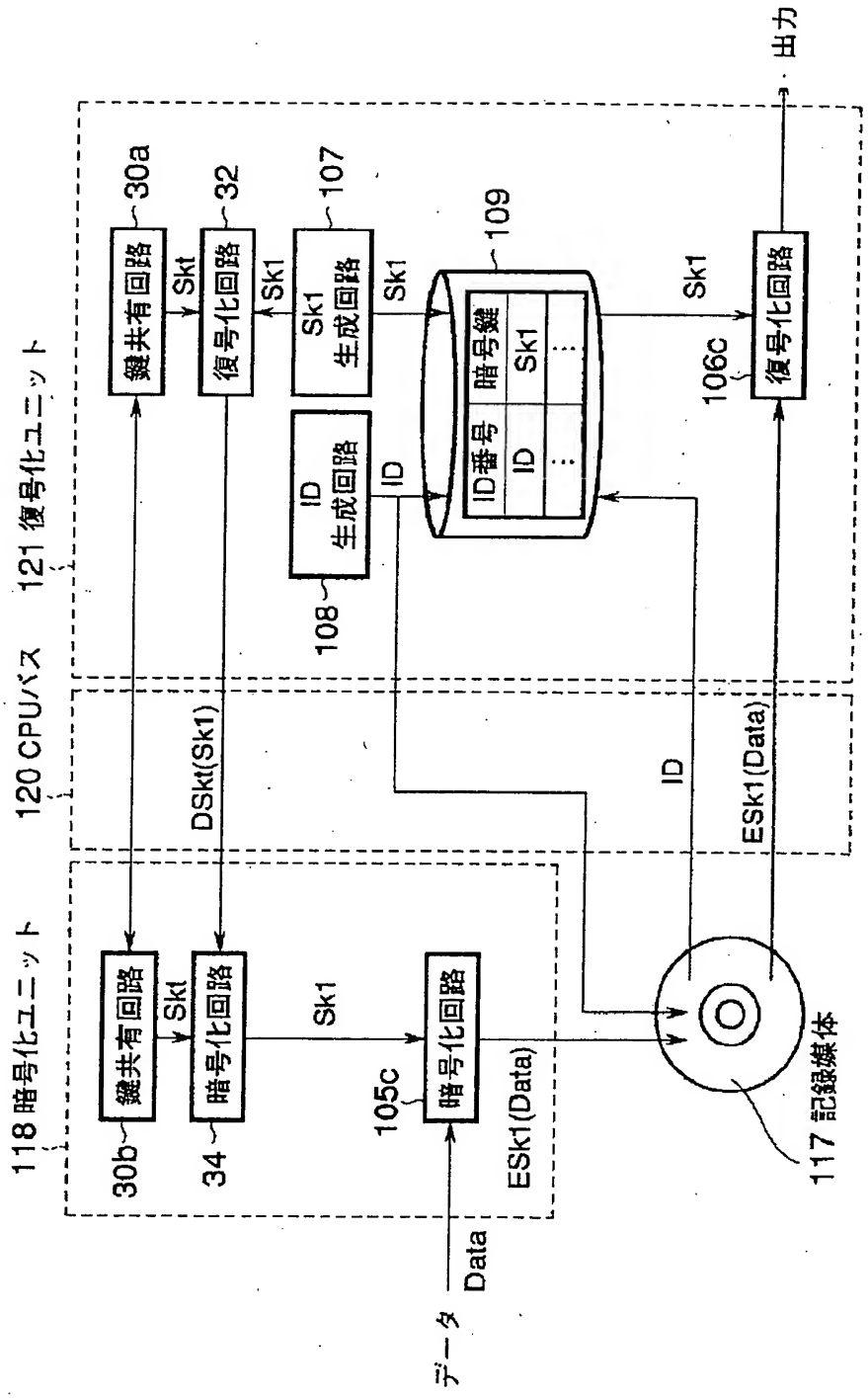
【符号の説明】

３０ａ，３０ｂ…鍵共有回路
３１ａ，３１ｂ…チャレンジ鍵生成回路
３３ａ，３３ｂ…認証鍵生成回路
３５ａ，３５ｂ…比較回路
３７ａ，３７ｂ…バス鍵生成回路
１０２ａ，１０２ｂ…マスター鍵の鍵束
１０５ａ～１０５ｃ…暗号化回路
１０６ａ～１０６ｄ…復号化回路
１０７…データ暗号鍵生成回路
１０８…ＩＤ生成回路
１０９…ＩＤ／鍵情報記憶回路
１１０…ＩＤ判定回路
１１７…記録媒体
１１８…暗号化ユニット
１２０…ＣＰＵバス
１２１…復号化ユニット
２１０…鍵判定回路

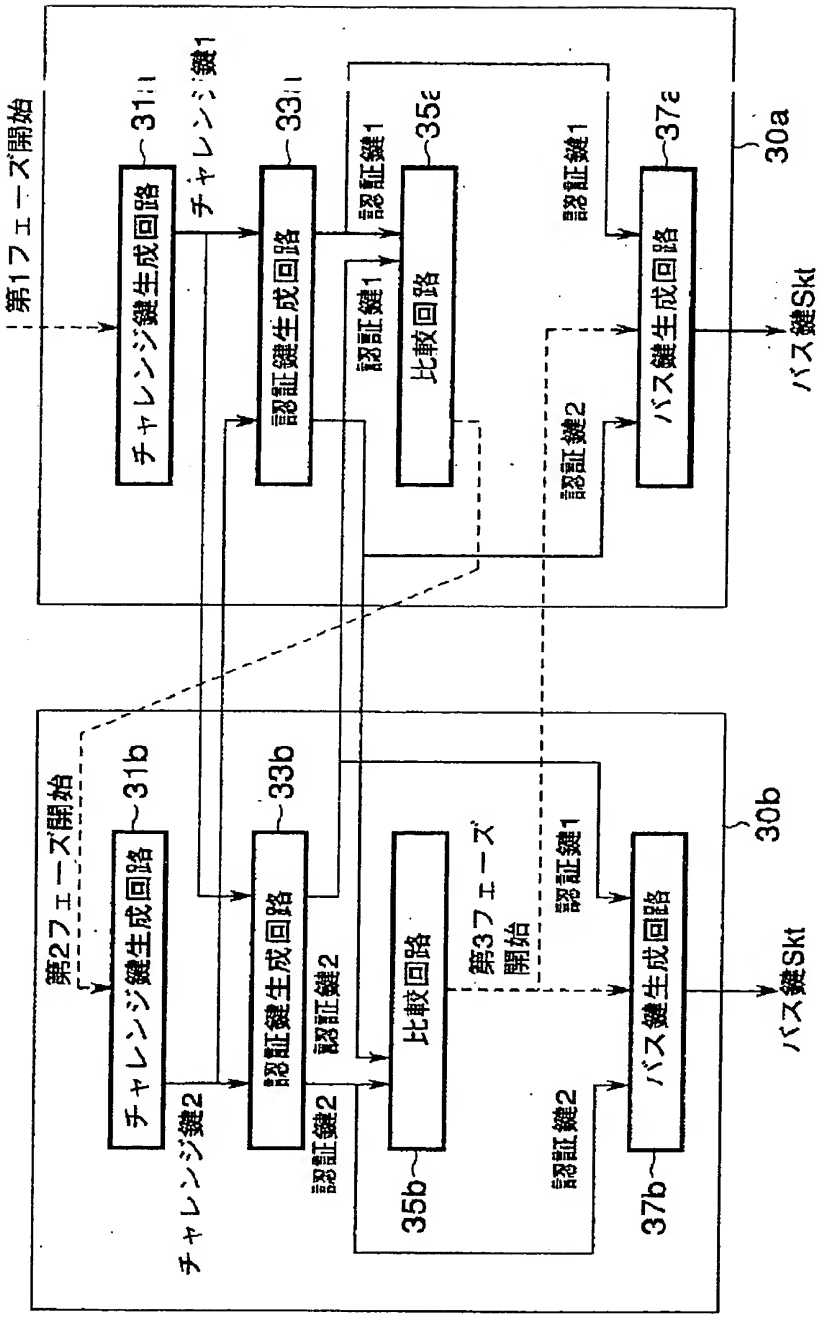
【図５】



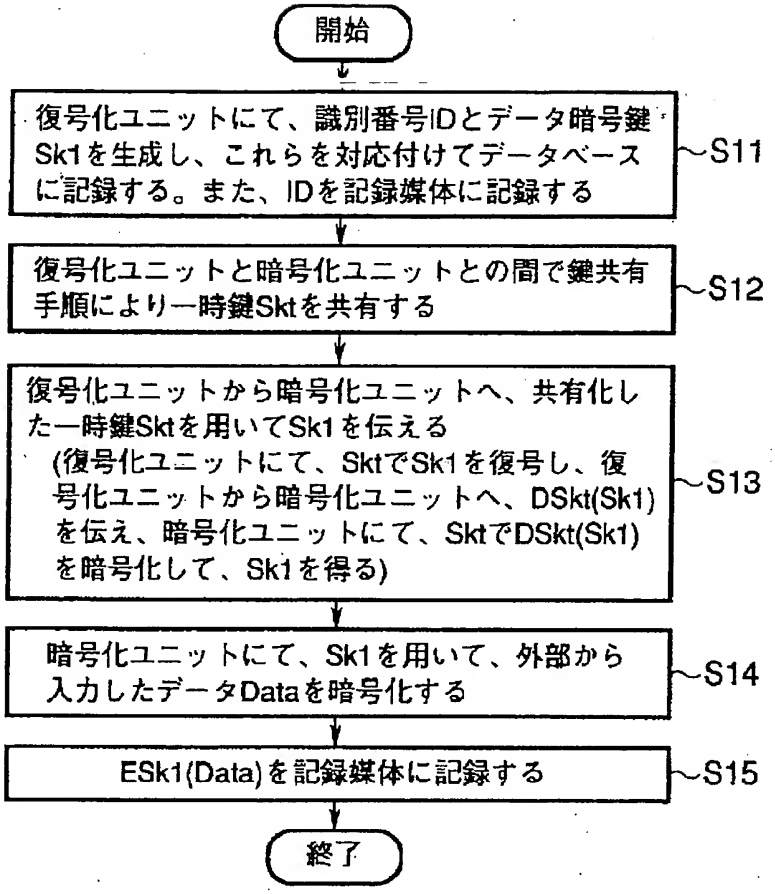
【図１】


出力
121 復号化ユニット
120 CPUバス
118 暗号化ユニット
30a
鍵共有回路
Skt
32
復号化回路
Sk1
107
Sk1
生成回路
Sk1
109
暗号鍵
Sk1
ID番号
ID
ID
生成回路
108
ID
106c
復号化回路
Sk1
DSkt(Sk1)
ID
ESk1(Data)
30b
鍵共有回路
Skt
34
暗号化回路
Sk1
105c
暗号化回路
ESk1(Data)
117 記録媒体
データ
Data

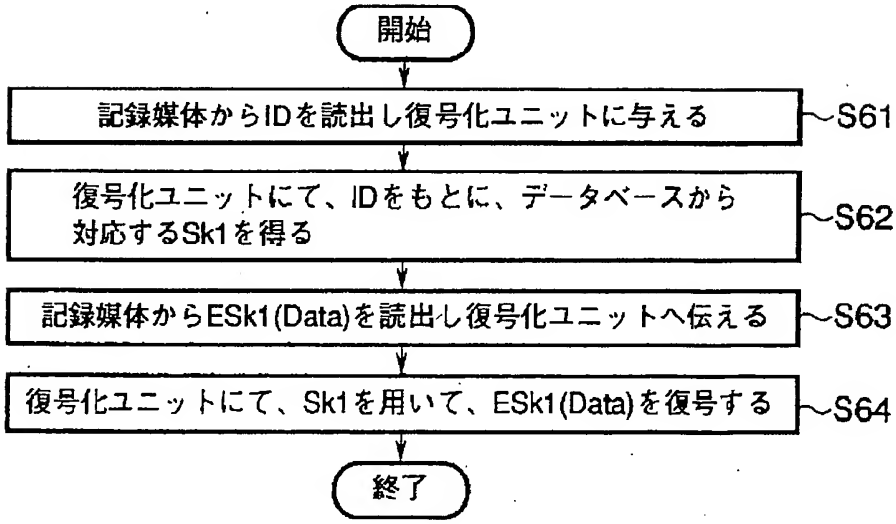
【図２】


第1フェーズ開始
チャレンジ鍵生成回路
31a
チャレンジ鍵1
認証鍵生成回路
33a
認証鍵1
比較回路
35a
認証鍵1
認証鍵2
バス鍵生成回路
37a
30a
バス鍵Skt
第2フェーズ開始
チャレンジ鍵生成回路
31b
チャレンジ鍵2
認証鍵生成回路
33b
認証鍵2
認証鍵2
比較回路
35b
第3フェーズ開始
認証鍵1
認証鍵2
バス鍵生成回路
37b
30b
バス鍵Skt

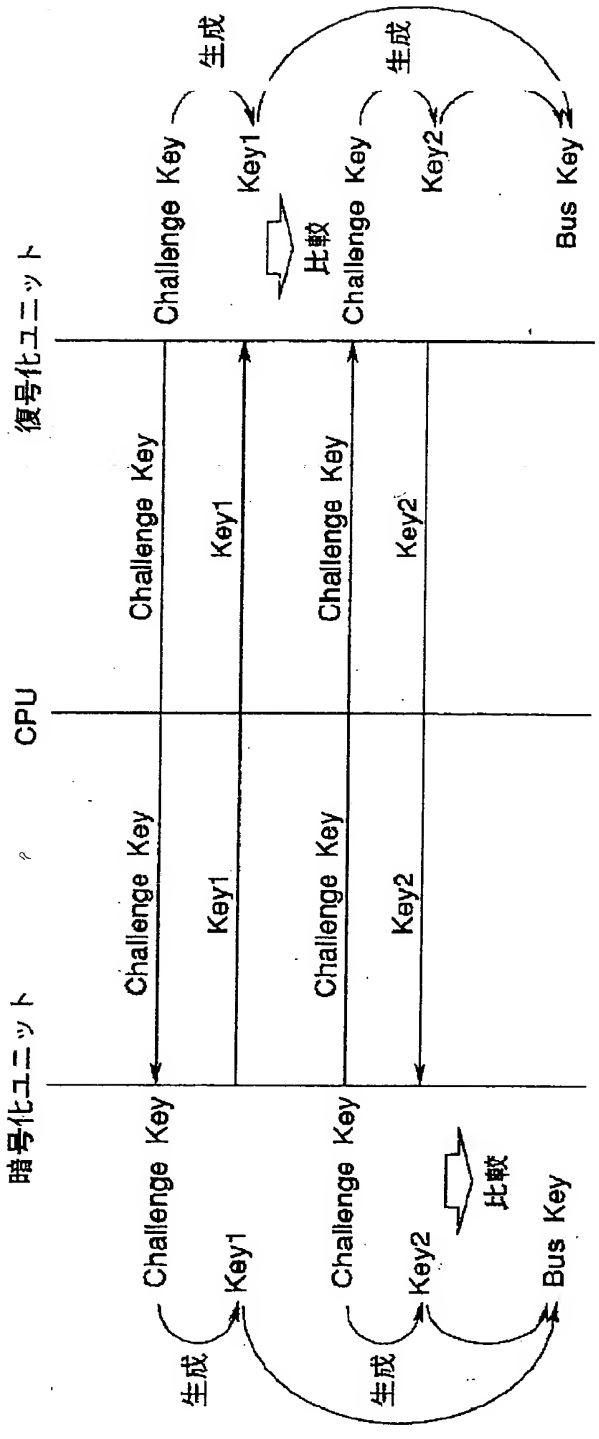
【図３】


開始
復号化ユニットにて、識別番号IDとデータ暗号鍵Sk1を生成し、これらを対応付けてデータベースに記録する。また、IDを記録媒体に記録する
S11
復号化ユニットと暗号化ユニットとの間で鍵共有手順により一時鍵Sktを共有する
S12
復号化ユニットから暗号化ユニットへ、共有化した一時鍵Sktを用いてSk1を伝える
(復号化ユニットにて、SktでSk1を復号し、復号化ユニットから暗号化ユニットへ、DSkt(Sk1)を伝え、暗号化ユニットにて、SktでDSkt(Sk1)を暗号化して、Sk1を得る)
S13
暗号化ユニットにて、Sk1を用いて、外部から入力したデータDataを暗号化する
S14
ESk1(Data)を記録媒体に記録する
S15
終了

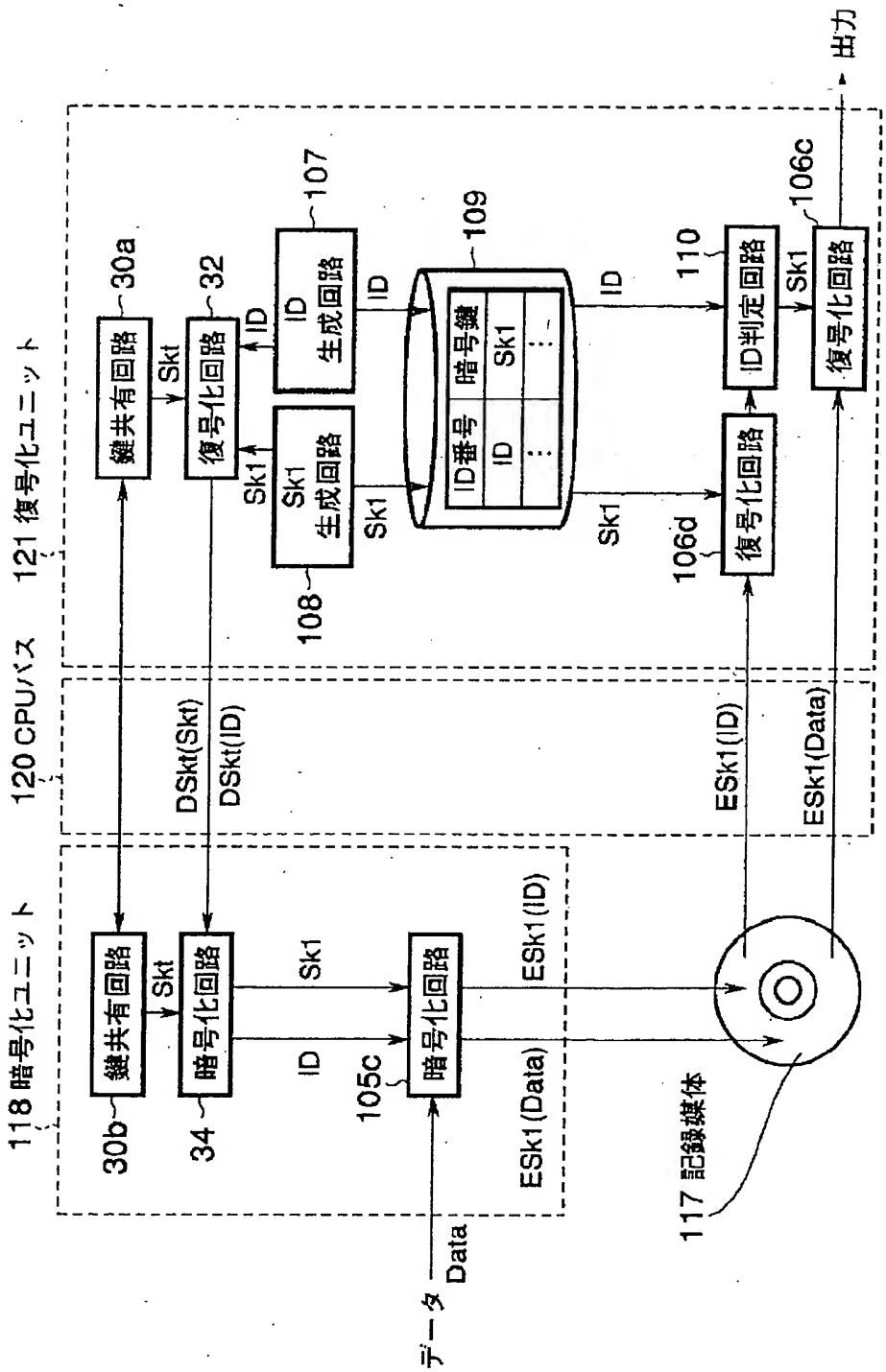
【図１１】


開始
記録媒体からIDを読出し復号化ユニットに与える
S61
復号化ユニットにて、IDをもとに、データベースから対応するSk1を得る
S62
記録媒体からESk1(Data)を読出し復号化ユニットへ伝える
S63
復号化ユニットにて、Sk1を用いて、ESk1(Data)を復号する
S64
終了

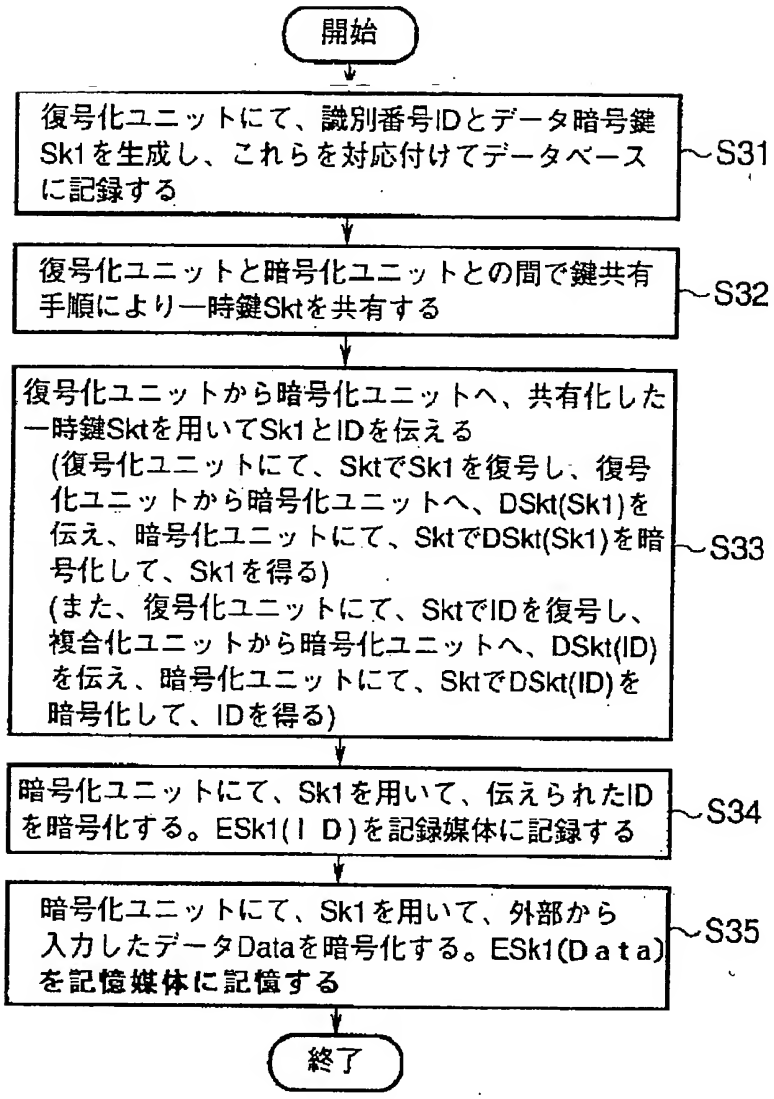
【図４】



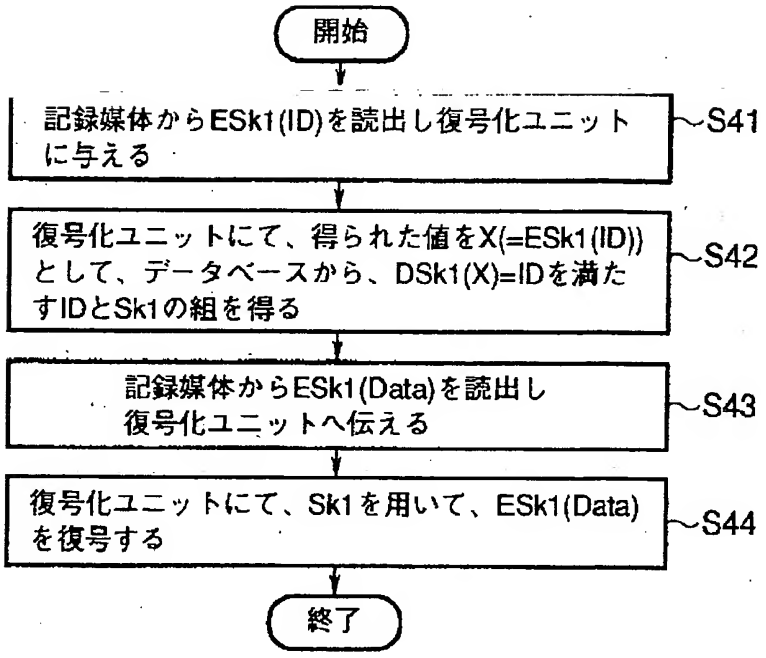
【図６】


出力
121 復号化ユニット
120 CPUバス
118 暗号化ユニット
30a
鍵共有回路
Skt
32
復号化回路
ID
107
ID
生成回路
109
ID番号
暗号鍵
ID
Sk1
108
Sk1
生成回路
Sk1
110
ID判定回路
106c
Sk1
復号化回路
106d
復号化回路
DSkt(Skt)
DSkt(ID)
ESk1(ID)
ESk1(Data)
30b
鍵共有回路
Skt
34
暗号化回路
Sk1
ID
105c
暗号化回路
ESk1(ID)
ESk1(Data)
117 記録媒体
データ
Data

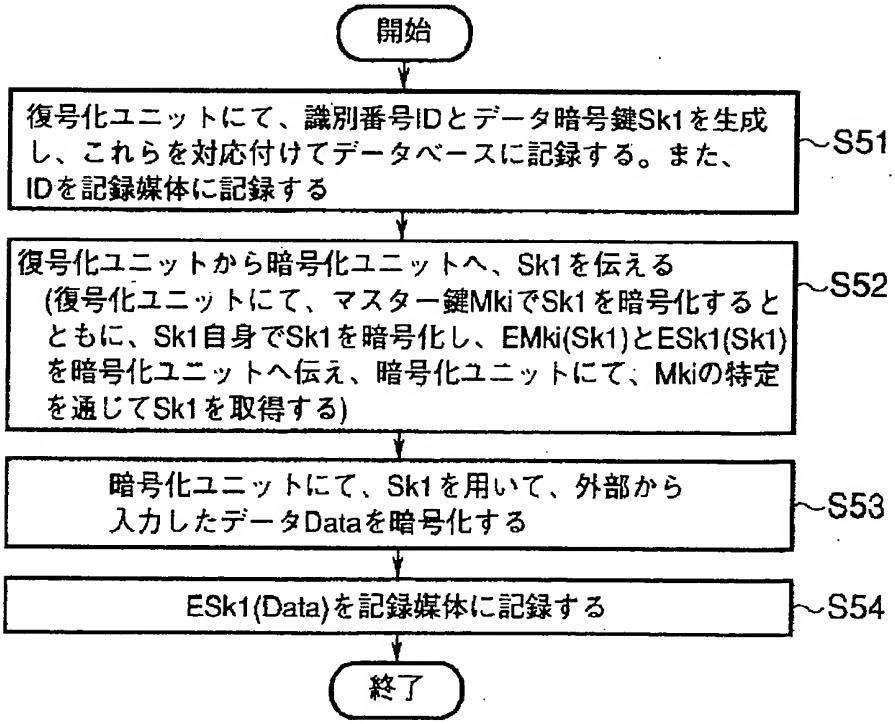
【図７】


開始
復号化ユニットにて、識別番号IDとデータ暗号鍵Sk1を生成し、これらを対応付けてデータベースに記録する
S31
復号化ユニットと暗号化ユニットとの間で鍵共有手順により一時鍵Sktを共有する
S32
復号化ユニットから暗号化ユニットへ、共有化した一時鍵Sktを用いてSk1とIDを伝える
(復号化ユニットにて、SktでSk1を復号し、復号化ユニットから暗号化ユニットへ、DSkt(Sk1)を伝え、暗号化ユニットにて、SktでDSkt(Sk1)を暗号化して、Sk1を得る)
(また、復号化ユニットにて、SktでIDを復号し、複合化ユニットから暗号化ユニットへ、DSkt(ID)を伝え、暗号化ユニットにて、SktでDSkt(ID)を暗号化して、IDを得る)
S33
暗号化ユニットにて、Sk1を用いて、伝えられたIDを暗号化する。ESk1(ＩＤ)を記録媒体に記録する
S34
暗号化ユニットにて、Sk1を用いて、外部から入力したデータDataを暗号化する。ESk1(Ｄａｔａ)を記憶媒体に記憶する
S35
終了

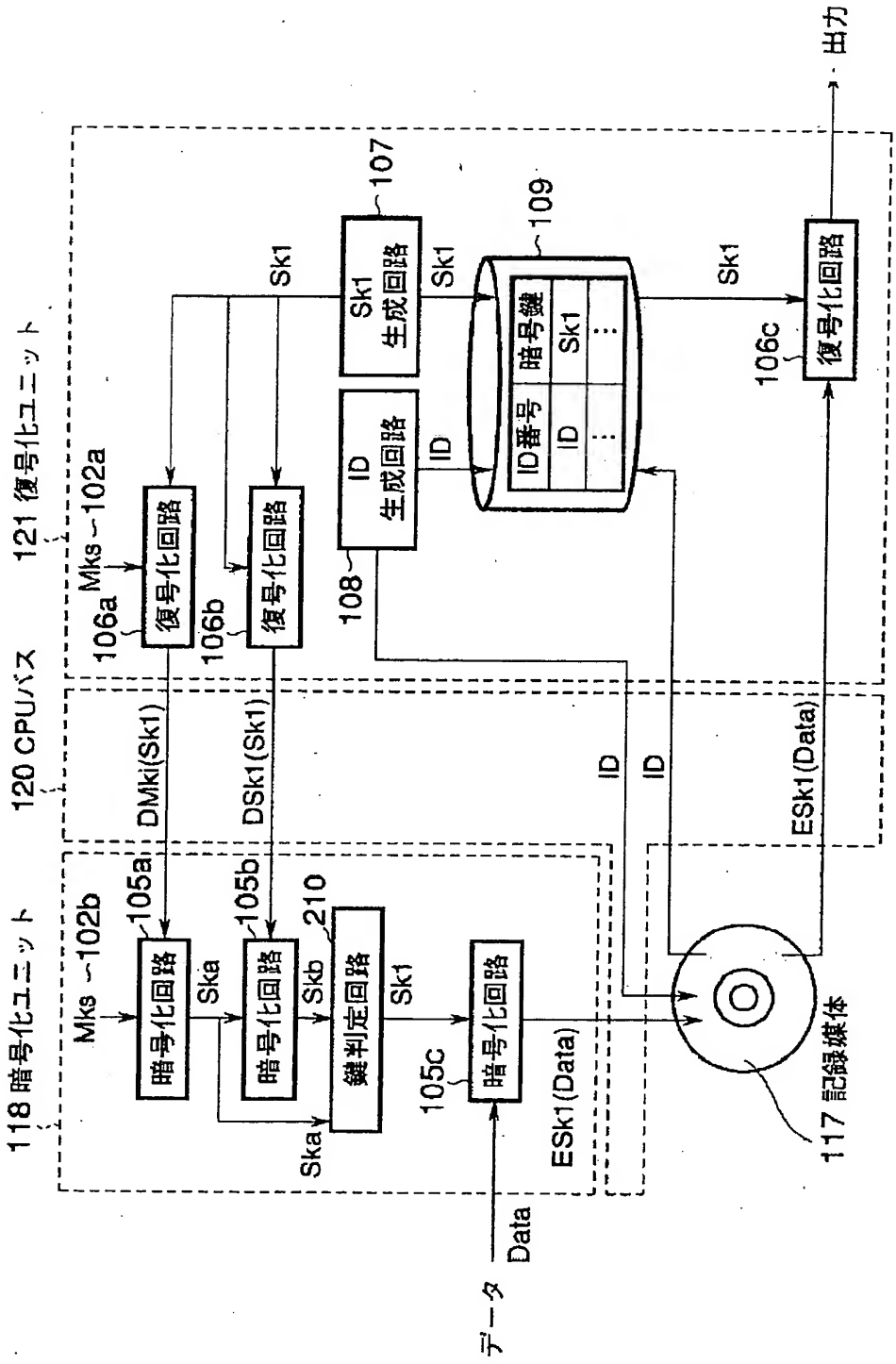
【図８】


開始
記録媒体からESk1(ID)を読出し復号化ユニットに与える
S41
復号化ユニットにて、得られた値をX(=ESk1(ID))として、データベースから、DSk1(X)=IDを満たすIDとSk1の組を得る
S42
記録媒体からESk1(Data)を読出し復号化ユニットへ伝える
S43
復号化ユニットにて、Sk1を用いて、ESk1(Data)を復号する
S44
終了

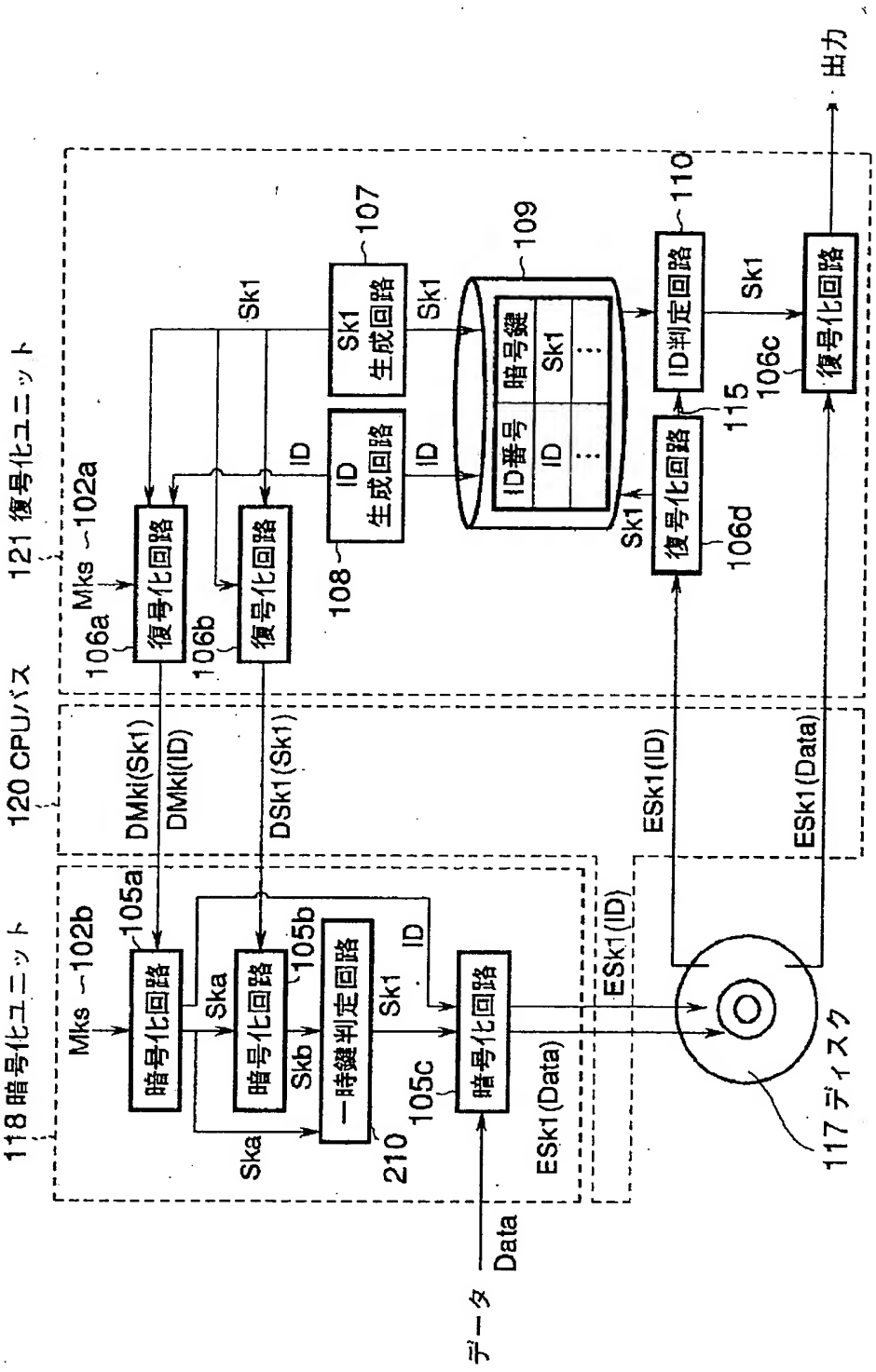
【図１０】


開始
復号化ユニットにて、識別番号IDとデータ暗号鍵Sk1を生成し、これらを対応付けてデータベースに記録する。また、IDを記録媒体に記録する
S51
復号化ユニットから暗号化ユニットへ、Sk1を伝える
(復号化ユニットにて、マスター鍵MkiでSk1を暗号化するとともに、Sk1自身でSk1を暗号化し、EMki(Sk1)とESk1(Sk1)を暗号化ユニットへ伝え、暗号化ユニットにて、Mkiの特定を通じてSk1を取得する)
S52
暗号化ユニットにて、Sk1を用いて、外部から入力したデータDataを暗号化する
S53
ESk1(Data)を記録媒体に記録する
S54
終了

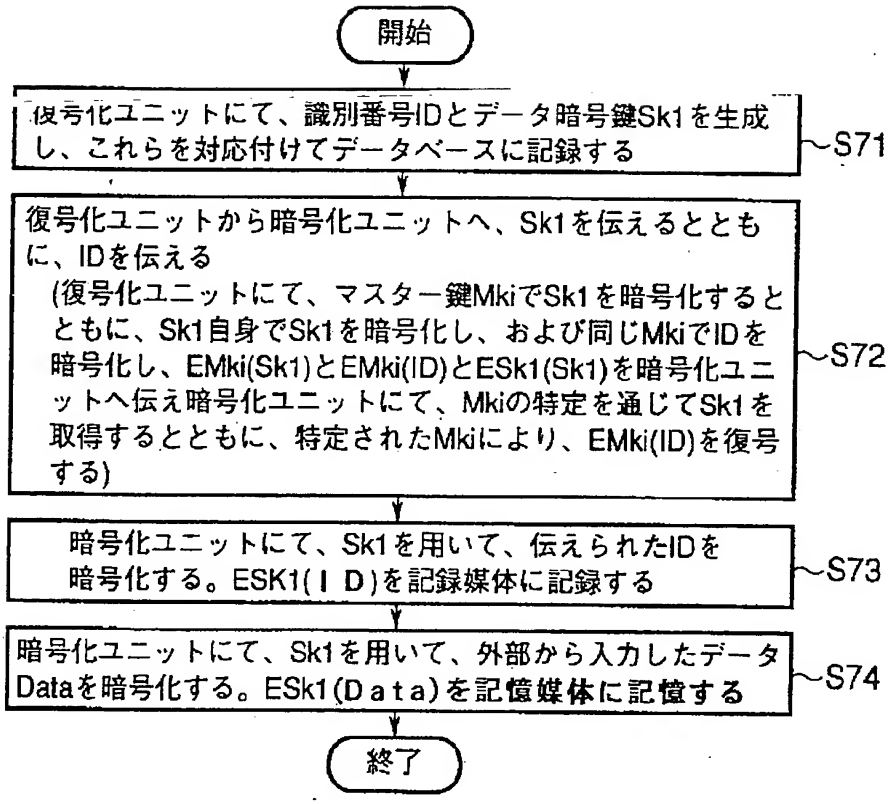
【図９】


118 暗号化ユニット
120 CPUバス
121 復号化ユニット
Mks
102b
102a
Mks
106a
106b
106c
復号化回路
復号化回路
復号化回路
105a
105b
105c
暗号化回路
暗号化回路
暗号化回路
210
鍵判定回路
107
Sk1
生成回路
108
ID
生成回路
109
ID番号
暗号鍵
ID
Sk1
DMki(Sk1)
DSk1(Sk1)
Ska
Skb
Sk1
Ska
Sk1
ID
ID
ESk1(Data)
ESk1(Data)
Data
データ
出力
117 記録媒体

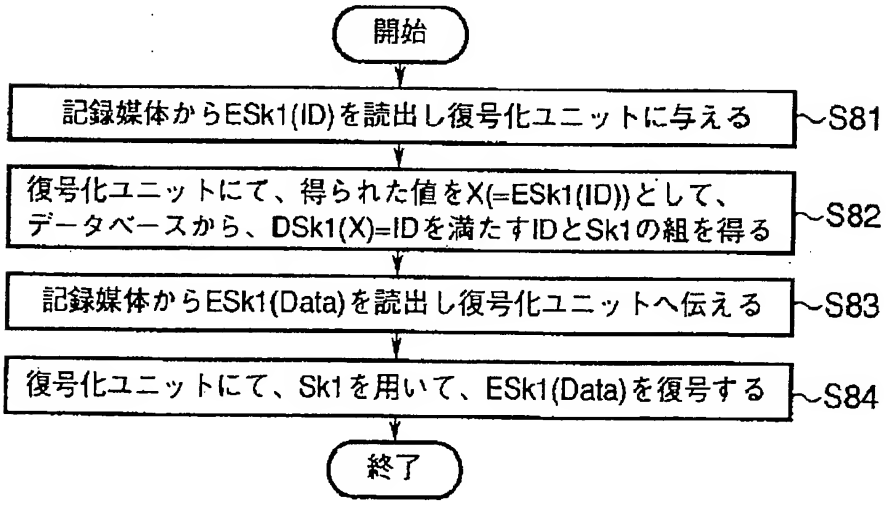
【図１２】


出力
121 復号化ユニット
120 CPUバス
118 暗号化ユニット
102a
102b
Mks
106a
復号化回路
106b
復号化回路
Sk1
107
Sk1 生成回路
108
ID 生成回路
ID
109
ID番号
暗号鍵
Sk1
110
ID判定回路
115
106c
復号化回路
106d
復号化回路
DMk(Sk1)
DMk(ID)
DSk1(Sk1)
ESk1(ID)
ESk1(Data)
105a
暗号化回路
105b
暗号化回路
Ska
Skb
一時鍵判定回路
210
105c
暗号化回路
ESk1(Data)
ESk1(ID)
117 ディスク
データ
Data

【図１３】


開始
復号化ユニットにて、識別番号IDとデータ暗号鍵Sk1を生成し、これらを対応付けてデータベースに記録する
S71
復号化ユニットから暗号化ユニットへ、Sk1を伝えるとともに、IDを伝える
(復号化ユニットにて、マスター鍵MkiでSk1を暗号化するとともに、Sk1自身でSk1を暗号化し、および同じMkiでIDを暗号化し、EMki(Sk1)とEMki(ID)とESk1(Sk1)を暗号化ユニットへ伝え暗号化ユニットにて、Mkiの特定を通じてSk1を取得するとともに、特定されたMkiにより、EMki(ID)を復号する)
S72
暗号化ユニットにて、Sk1を用いて、伝えられたIDを暗号化する。ESK1(ＩＤ)を記録媒体に記録する
S73
暗号化ユニットにて、Sk1を用いて、外部から入力したデータDataを暗号化する。ESk1(Ｄａｔａ)を記憶媒体に記憶する
S74
終了

【図１４】


開始
記録媒体からESk1(ID)を読出し復号化ユニットに与える
S81
復号化ユニットにて、得られた値をX(=ESk1(ID))として、データベースから、DSk1(X)=IDを満たすIDとSk1の組を得る
S82
記録媒体からESk1(Data)を読出し復号化ユニットへ伝える
S83
復号化ユニットにて、Sk1を用いて、ESk1(Data)を復号する
S84
終了